PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-344537
(43)Date of publication of application : 14.12.2001

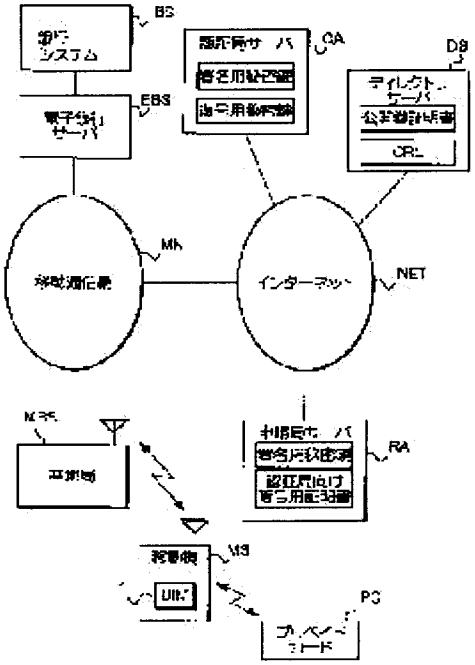
(51)Int.Cl. G06F 17/60

(21)Application number : 2000-163676
(22)Date of filing : 31.05.2000

(71)Applicant : NTT DOCOMO INC
(72)Inventor : KINOSHITA MAKI
YAMASHITA TETSUYA

(54) ELECTRONIC VALUE SYSTEM, COMMUNICATION TERMINAL AND SERVER

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an electronic value system which secures security and also improves performance.
SOLUTION: An electronic bank server EBS stores an electronic value amount stored in an UIM 1 in a mobile machine MS together with an electronic value amount in an electronic account and updates the electronic value amounts in accordance with the contents of a transaction made by using an electronic value.



* NOTICES *

JPO and INPIT are not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1]An electronic value system which is provided with the following and characterized by basing said wallet balance management tool on said transaction log notified, and memorizing and updating balance information of said electronic value.
Electronic account holding mechanism which is an electronic value system which manages an electronic value which is electronic money information, was provided in a server on a network, and was assigned to each of two or more users and which accumulates said electronic value for every electronic account.
A memory which stores said electronic value.
Two or more communication terminals which have a means of communication which transmits and receives said electronic value, and are used as said user's electronic purse between external nodes.
A download means which downloads said electronic value in a memory of said communication terminal via said network from said electronic account holding mechanism, A wallet balance management tool which memorizes balance information of an electronic value which is provided on said network and stored in a memory of said communication terminal, and is updated, A transaction log reporting means which notifies a transaction log which shows the contents of dealings using said electronic value from said communication terminal via said network to said wallet balance management tool.

[Claim 2]In the electronic value system according to claim 1, said two or more communication terminals, Said electronic value including the 1st communication terminal and 2nd communication terminal that are transmitted and received mutually a means of communication of said 1st communication terminal, Transmit to said 2nd communication terminal with an electronic value stored in said memory, and self identification information a means of communication of said 2nd communication terminal, While receiving identification information of an electronic value transmitted from said 1st communication terminal, and said 1st communication terminal, transmit to said 1st communication terminal and self identification information said transaction log reporting means, Among the 1st communication terminal or said 2nd communication terminal, from either to said wallet balance management tool at least A frame of said electronic value transmitted and received, An electronic value system, wherein it transmits identification information of said 1st communication terminal and said 2nd communication terminal as said transaction log and said wallet balance management tool updates balance information of said electronic value based on said transaction log transmitted.
[Claim 3]In the electronic value system according to claim 2, said 1st communication terminal and said 2nd communication terminal, Have a log accumulation means which accumulates said transaction log concerning own dealings, and at least among said 1st communication terminal or said 2nd communication terminal either, An electronic value system which will be characterized by not performing transmission and reception of an external node and an electronic value if said transaction log equivalent to a storage capacity by said log accumulation means is accumulated.
[Claim 4]In the electronic value system according to claim 2, said 1st communication terminal and

said 2nd communication terminal, Have a log accumulation means which accumulates said transaction log concerning own dealings, and at least among said 1st communication terminal or said 2nd communication terminal either, An electronic value system eliminating said transaction log from old order at the time of a trade date at the time of dealings after it if said transaction log equivalent to a storage capacity by said log accumulation means is accumulated.
[Claim 5]In the electronic value system according to claim 2, said 1st communication terminal and said 2nd communication terminal, Have a log accumulation means which accumulates said transaction log concerning own dealings, and said transaction log reporting means, An electronic value system which will be characterized by transmitting the transaction log concerned to said wallet balance management tool if said transaction log which is equivalent to a storage capacity by said log accumulation means in either at least among said 1st communication terminal or said 2nd communication terminal is accumulated.
[Claim 6]An electronic value system, wherein said communication terminal is a mobile communication terminal accommodated in a mobile radio communication network in the electronic value system according to claim 1 and said network is said mobile radio communication network.
[Claim 7]In the electronic value system according to any one of claims 2 to 5, said communication terminal, An electronic value system which it is a mobile communication terminal accommodated in a mobile radio communication network, and said network is said mobile radio communication network, and is characterized by a means of communication of said 1st communication terminal and a means of communication of the 2nd communication terminal communicating by radio.
[Claim 8]An electronic value system, wherein said communication terminal is a mobile communication terminal accommodated in a mobile radio communication network in the electronic value system according to claim 1 and a memory of said communication terminal is an IC card used equipping the communication terminal concerned.
[Claim 9]An electronic value system comprising:
It is an electronic value system which transmits and receives an electronic value which is electronic money information between the 1st communication terminal and the 2nd communication terminal, and said 1st communication terminal is said electronic value.
Identification information of an issue subject who published the electronic value concerned.
A memory which stores an electronic signature performed by said issue subject to the identification information concerned.
With said electronic value stored, have a transmitting means for transmitting said issue subject's identification information and an electronic signature to said 2nd communication terminal, and said 2nd communication terminal, A reception means which receives said issue subject's identification information and an electronic signature with an electronic value transmitted from said 1st communication terminal, and by verifying said received electronic signature, A decision means which checks what an electronic value transmitted from said 1st communication terminal was published for by said issue subject, and judges the justification of said 1st communication terminal by this.

[Claim 10]An electronic value system comprising:
In the electronic value system according to claim 9, said 2nd communication terminal is said electronic value.
Identification information of an issue subject who published the electronic value concerned.
A memory which stores an electronic signature performed by said issue subject to the identification information concerned.
Have a transmitting means for transmitting identification information and an electronic signature of said said issue subject stored to said 1st communication terminal, and said 1st communication terminal, An acquisition means which acquires an electronic signature performed by said issue subject to said issue subject's identification information and identification information concerned in a memory of said 2nd communication terminal before transmitting said electronic value to said 2nd communication terminal, A decision means which checks what an electronic value in a memory of said 2nd communication terminal was published for by said issue subject by verifying said acquired electronic signature, and judges the justification of said 2nd communication terminal by this.

[Claim 11]In the electronic value system according to claim 9 or 10, said 1st communication terminal and said 2nd communication terminal, Have a log accumulation means which accumulates said transaction log concerning own dealings, and at least among said 1st communication terminal or said 2nd communication terminal either, An electronic value system transmitting said accumulated transaction log to an external node which has managed balance information of an electronic value which self has memorized if said transaction log equivalent to a storage capacity by said log accumulation means is accumulated.
[Claim 12]An electronic value system, wherein said 1st communication terminal and said 2nd communication terminal transmit and receive an electronic value by radio in the electronic value system according to any one of claims 9 to 11.
[Claim 13]An electronic value system characterized by being a mobile communication terminal of said 1st communication terminal or said 2nd communication terminal which is accommodated in a mobile radio communication network as for either at least in the electronic value system according to any one of claims 9 to 12.
[Claim 14]An electronic value system, wherein said 2nd communication terminal is built in a vending machine which sells goods in the electronic value system according to any one of claims 9 to 13.
[Claim 15]An electronic value system when said communication terminal transmits said electronic value outside in the electronic value system according to any one of claims 1 to 14, wherein it adds the transmission date to the electronic value concerned and transmits.
[Claim 16]The electronic value system comprising according to claim 1 to 15:
A security means which performs processing of electronic authentication, and a code and decoding using a key to the electronic value concerned when said communication terminal transmits and receives the exterior and said electronic value.
An update means which updates said key periodically.

[Claim 17]A communication terminal which is provided with the following, and will be characterized by not transmitting and receiving said electronic value between said external nodes if said transaction log equivalent to a storage capacity by said log accumulation means is accumulated.
A memory which stores an electronic value and self identification information which are electronic money information.
A means of communication which transmits and receives said electronic value between external nodes.
An identification information means of exchange which acquires identification information of said external node to the external node concerned while giving self identification information stored in said memory to said external node.
A log accumulation means which accumulates a frame of said electronic value transmitted and received between said external nodes, and said self identification information and identification information of said external node as a transaction log.

[Claim 18]A communication terminal which is provided with the following, and will be characterized by eliminating said transaction log accumulated from old order of transmission and reception date and time at the time of transmission and reception of said electronic value after it if said transaction log equivalent to a storage capacity by said log accumulation means is accumulated.
A memory which stores an electronic value and self identification information which are electronic money information.
A means of communication which transmits and receives said electronic value between external nodes.
An identification information means of exchange which acquires identification information of said external node to the external node concerned while giving self identification information stored in said memory to said external node.
A log accumulation means which accumulates a frame of said electronic value transmitted and received between said external nodes, and said self identification information and identification

information of said external node as a transaction log with transmission and reception date and time.

[Claim 19]A communication terminal which is provided with the following and characterized by transmitting said transaction log accumulated to an external device which checks justification about transmission and reception of said electronic value using the transaction log concerned if said transaction log equivalent to a storage capacity by said log accumulation means is accumulated.
A memory which stores an electronic value and self identification information which are electronic money information.
A means of communication which transmits and receives said electronic value between external nodes.
An identification information means of exchange which acquires identification information of said external node to the external node concerned while giving self identification information stored in said memory to said external node.
A log accumulation means which accumulates a frame of said electronic value transmitted and received between said external nodes, and said self identification information and identification information of said external node as a transaction log with transmission and reception date and time.

[Claim 20]A communication terminal comprising:
An electronic value which is electronic money information.
Identification information of an issue subject of the electronic value concerned.
A memory which stores an electronic signature performed by said issue subject to the identification information concerned.
A means of communication which transmits and receives said electronic value between external nodes, and an addition means which adds said issue subject's identification information and said electronic signature to an electronic value transmitted to said external node by said means of communication, A verifying means which checks the justification of said electronic value by verifying identification information and said electronic signature of said issue subject added to an electronic value which received from said external node by said means of communication.

[Claim 21]The communication terminal comprising according to claim 17 to 20:
A security means which performs processing of electronic authentication, and a code and decoding using a key to the electronic value concerned when said communication terminal transmits and receives the exterior and said electronic value.
An update means which updates said key periodically.

[Claim 22]A communication terminal adding the transmission date to said electronic value, and transmitting in the communication terminal according to any one of claims 17 to 21 when transmitting said electronic value to said external node.
[Claim 23]A communication terminal, wherein said means of communication transmits in the communication terminal according to any one of claims 17 to 22 and receives said electronic value between said external nodes by radio.
[Claim 24]A communication terminal, wherein said communication terminal is a mobile communication terminal accommodated in a mobile radio communication network in the communication terminal according to any one of claims 17 to 23 and said memory is an IC card used equipping the communication terminal concerned.
[Claim 25]A server which memorizes an electronic value which is electronic money information, comprising:
Electronic account holding mechanism which was assigned to a user and which accumulates said electronic value for every electronic account.
A memory which stores said electronic value.
A download means which downloads an electronic value accumulated by said electronic account

holding mechanism to a communication terminal with a means of communication which transmits and receives said electronic value between external nodes via said network.
A wallet balance memory measure which memorizes balance information of an electronic value stored in a memory of said communication terminal, A log acquisition means to acquire a transaction log which shows the contents of dealings using said electronic value in said communication terminal from said communication terminal via said network, A wallet balance update means which updates balance information of said electronic value memorized by said wallet balance memory measure based on said acquired transaction log.

[Claim 26]A server provided with an electronic authentication means to be the server according to claim 25 and to perform electronic authentication with a key which self memorizes to said electronic value information to download.

[Translation done.]

* NOTICES *

JPO and INPIT are not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention relates to the electronic value system, communication terminal, and server for performing electronic commerce technology using an electronic value.
[0002]
[Description of the Prior Art]The system for performing cashless payment shopping is proposed [various] using electronic money information (it is hereafter called an electronic value).
[0003]
[Problem(s) to be Solved by the Invention]By the way, this electronic value has a possibility that injustice, such as becoming the alteration of the data itself and an owner of an electronic value, and clearing up since it is only mere data, may occur, and the security reservation for preventing this has been a technical problem. On the other hand, operating the system for security reservation also means that the processing for it increases, and it becomes a factor which degrades the processing efficiency of the whole system. The purpose of this invention is as follows. Be made in view of such a background and secure security.
Provide the electronic value system, communication terminal, and server which raise processing efficiency.

[0004]
[Means for Solving the Problem]In order to solve a technical problem mentioned above, the invention according to claim 1, It is an electronic value system which manages an electronic value which is electronic money information, Electronic account holding mechanism which was provided in a server on a network and assigned to each of two or more users and which accumulates said electronic value for every electronic account, Two or more communication terminals which have a memory which stores said electronic value, and a means of communication which transmits and receives said electronic value between external nodes, and are used as said user's electronic purse, A download means which downloads said electronic value in a memory of said communication terminal via said network from said electronic account holding mechanism, A wallet balance management tool which memorizes balance information of an electronic value which is provided on said network and stored in a memory of said communication terminal, and is updated, From said communication terminal via said network to said wallet balance management tool, It has a transaction log reporting means which notifies a transaction log which shows the contents of dealings using said electronic value, said wallet balance management tool is based on said transaction log notified, and balance information of said electronic value is memorized and updated.

[0005]In the electronic value system according to claim 1, the invention according to claim 2 said two or more communication terminals, Said electronic value including the 1st communication terminal and 2nd communication terminal that are transmitted and received mutually a means of communication of said 1st communication terminal, Transmit to said 2nd communication terminal with an electronic value stored in said memory, and self identification information a means of communication of said 2nd communication terminal, While receiving identification information of an

electronic value transmitted from said 1st communication terminal, and said 1st communication terminal, transmit to said 1st communication terminal and self identification information said transaction log reporting means, Among the 1st communication terminal or said 2nd communication terminal, from either to said wallet balance management tool at least A frame of said electronic value transmitted and received, Transmitting identification information of said 1st communication terminal and said 2nd communication terminal as said transaction log, said wallet balance management tool updates balance information of said electronic value based on said transaction log transmitted.

[0006]In the electronic value system according to claim 2, the invention according to claim 3 said 1st communication terminal and said 2nd communication terminal, Have a log accumulation means which accumulates said transaction log concerning own dealings, and at least among said 1st communication terminal or said 2nd communication terminal either, Accumulation of said transaction log equivalent to a storage capacity by said log accumulation means will not perform transmission and reception of an external node and an electronic value.

[0007]In the electronic value system according to claim 2, the invention according to claim 4 said 1st communication terminal and said 2nd communication terminal, Have a log accumulation means which accumulates said transaction log concerning own dealings, and at least among said 1st communication terminal or said 2nd communication terminal either, At the time of dealings after it, accumulation of said transaction log equivalent to a storage capacity by said log accumulation means will eliminate said transaction log from old order at the time of a trade date.

[0008]In the electronic value system according to claim 2, the invention according to claim 5 said 1st communication terminal and said 2nd communication terminal, Have a log accumulation means which accumulates said transaction log concerning own dealings, and said transaction log reporting means, Accumulation of said transaction log which is equivalent to a storage capacity by said log accumulation means in either at least among said 1st communication terminal or said 2nd communication terminal will transmit the transaction log concerned to said wallet balance management tool.

[0009]The invention according to claim 6 is a mobile communication terminal in which said communication terminal is accommodated in a mobile radio communication network in the electronic value system according to claim 1, and said network is characterized by being said mobile radio communication network.

[0010]In the electronic value system according to any one of claims 2 to 5, the invention according to claim 7 said communication terminal, It is a mobile communication terminal accommodated in a mobile radio communication network, said network is said mobile radio communication network, and a means of communication of said 1st communication terminal and a means of communication of the 2nd communication terminal communicate by radio.

[0011]The invention according to claim 8 is a mobile communication terminal in which said communication terminal is accommodated in a mobile radio communication network in the electronic value system according to claim 1, and a memory of said communication terminal is characterized by being an IC card used equipping the communication terminal concerned.

[0012]The invention according to claim 9 between the 1st communication terminal and the 2nd communication terminal, Are an electronic value which is electronic money information an electronic value system transmitted and received, and said 1st communication terminal, With a memory which stores said electronic value, identification information of an issue subject who published the electronic value concerned, and an electronic signature performed by said issue subject to the identification information concerned, and said electronic value stored. Have a transmitting means for transmitting said issue subject's identification information and an electronic signature to said 2nd communication terminal, and said 2nd communication terminal, A reception means which receives said issue subject's identification information and an electronic signature with an electronic value transmitted from said 1st communication terminal, and by verifying said received electronic signature, What an electronic value transmitted from said 1st communication terminal was published for by said issue subject is checked, and this is provided with a decision means which judges the justification of said 1st communication terminal.

[0013]In the electronic value system according to claim 9, the invention according to claim 10 said

2nd communication terminal, Said electronic value and identification information of an issue subject who published the electronic value concerned, A memory which stores an electronic signature performed by said issue subject to the identification information concerned, Have a transmitting means for transmitting identification information and an electronic signature of said said issue subject stored to said 1st communication terminal, and said 1st communication terminal, An acquisition means which acquires an electronic signature performed by said issue subject to said issue subject's identification information and identification information concerned in a memory of said 2nd communication terminal before transmitting said electronic value to said 2nd communication terminal, By verifying said acquired electronic signature, what an electronic value in a memory of said 2nd communication terminal was published for by said issue subject is checked, and this is provided with a decision means which judges the justification of said 2nd communication terminal.

[0014]In the electronic value system according to claim 9 or 10, the invention according to claim 11 said 1st communication terminal and said 2nd communication terminal, Have a log accumulation means which accumulates said transaction log concerning own dealings, and at least among said 1st communication terminal or said 2nd communication terminal either, Accumulation of said transaction log equivalent to a storage capacity by said log accumulation means will transmit said accumulated transaction log to an external node which has managed balance information of an electronic value which self has memorized.

[0015]In the electronic value system according to any one of claims 9 to 11, said 1st communication terminal and said 2nd communication terminal transmit [the invention according to claim 12] and receive an electronic value by radio.

[0016]The invention according to claim 13 is characterized by either being a mobile communication terminal of said 1st communication terminal or said 2nd communication terminal accommodated in a mobile radio communication network at least in the electronic value system according to any one of claims 9 to 12.

[0017]The invention according to claim 14 is built in a vending machine in which said 2nd communication terminal sells goods in the electronic value system according to any one of claims 9 to 13.

[0018]In the electronic value system according to any one of claims 1 to 14, said communication terminal adds the transmission date to the electronic value concerned, and the invention according to claim 15 transmits it, when transmitting said electronic value outside.

[0019]In the electronic value system according to claim 1 to 15, the invention according to claim 16 said communication terminal, An electronic value system having a security means which performs processing of electronic authentication, and a code and decoding using a key to the electronic value concerned, and an update means which updates said key periodically when transmitting and receiving the exterior and said electronic value.

[0020]A memory which stores an electronic value and self identification information which are money information with the electronic invention according to claim 17, A means of communication which transmits and receives said electronic value between external nodes, and an identification information means of exchange which acquires identification information of said external node to the external node concerned while giving self identification information stored in said memory to said external node, It has a log accumulation means which accumulates a frame of said electronic value transmitted and received between said external nodes, and said self identification information and identification information of said external node as a transaction log, Accumulation of said transaction log equivalent to a storage capacity by said log accumulation means will not transmit and receive said electronic value between said external nodes.

[0021]A memory which stores an electronic value and self identification information which are money information with the electronic invention according to claim 18, A means of communication which transmits and receives said electronic value between external nodes, and an identification information means of exchange which acquires identification information of said external node to the external node concerned while giving self identification information stored in said memory to said external node, A frame of said electronic value transmitted and received between said external nodes, and said self identification information and identification information of said external node, If

said transaction log which is provided with a log accumulation means accumulated as a transaction log with transmission and reception date and time, and is equivalent to a storage capacity by said log accumulation means is accumulated, At the time of transmission and reception of said electronic value after it, said transaction log accumulated is eliminated from old order of transmission and reception date and time.
[0022]A memory which stores an electronic value and self identification information which are money information with the electronic invention according to claim 19, A means of communication which transmits and receives said electronic value between external nodes, and an identification information means of exchange which acquires identification information of said external node to the external node concerned while giving self identification information stored in said memory to said external node, A frame of said electronic value transmitted and received between said external nodes, and said self identification information and identification information of said external node, If said transaction log which is provided with a log accumulation means accumulated as a transaction log with transmission and reception date and time, and is equivalent to a storage capacity by said log accumulation means is accumulated, Said transaction log accumulated is transmitted to an external device which checks justification about transmission and reception of said electronic value using the transaction log concerned.
[0023]written this invention is characterized by it having been alike and comprising the following at claim 20.
An electronic value which is electronic money information.
Identification information of an issue subject of the electronic value concerned.
A memory which stores an electronic signature performed by said issue subject to the identification information concerned.
A means of communication which transmits and receives said electronic value between external nodes, and an addition means which adds said issue subject's identification information and said electronic signature to an electronic value transmitted to said external node by said means of communication, A verifying means which checks the justification of said electronic value by verifying identification information and said electronic signature of said issue subject added to an electronic value which received from said external node by said means of communication.

[0024]In the communication terminal according to claim 17 to 20, the invention according to claim 21 said communication terminal, A security means which performs processing of electronic authentication, and a code and decoding using a key to the electronic value concerned when transmitting and receiving the exterior and said electronic value, It has an update means which updates said key periodically. The invention according to claim 21, In the communication terminal according to any one of claims 17 to 20, when transmitting said electronic value to said external node, the transmission date is added to said electronic value, and it transmits.
[0025]Said means of communication transmits [the invention according to claim 23] in the communication terminal according to any one of claims 17 to 22 and receives said electronic value between said external nodes by radio. [0026]The invention according to claim 24 is a mobile communication terminal in which said communication terminal is accommodated in a mobile radio communication network in the communication terminal according to any one of claims 17 to 23, and said memory is characterized by being an IC card used equipping the communication terminal concerned.
[0027]The invention according to claim 25 is provided with the following.
Electronic account holding mechanism which is a server which memorizes an electronic value which is electronic money information, and was assigned to a user and which accumulates said electronic value for every electronic account.
A memory which stores said electronic value.
A download means which downloads an electronic value accumulated by said electronic account holding mechanism to a communication terminal with a means of communication which transmits and receives said electronic value between external nodes via said network, A wallet balance memory measure which memorizes balance information of an electronic value stored in a memory of said communication terminal, A log acquisition means to acquire a transaction log which shows

the contents of dealings using said electronic value in said communication terminal from said communication terminal via said network, A wallet balance update means which updates balance information of said electronic value memorized by said wallet balance memory measure based on said acquired transaction log.
The invention according to claim 26 is provided with an electronic authentication means to be the server according to claim 25 and to perform electronic authentication with a key which self memorizes to said electronic value information to download.
[0028]
[Embodiment of the Invention]Hereafter, an embodiment of the invention is described, referring to drawings. According to this embodiment, while establishing each user's electronic account to the electronic bank provided on the network, the moving machine which each user possesses is used as an electronic purse. Suppose that the electronic authentication based on the RSA public-key crypto system of a PKI (Public Key Infrastructure) base and the function of a code and decoding are utilized in the exchange of this electronic value.
[0029]A: **** -- explain the composition of an embodiment first. Drawing 1 is a block diagram showing the composition of the whole system concerning an embodiment. As shown in the figure, this system comprises moving machine MS, the mobile radio communication network MN, prepaid card PC, the electronic bank server Electronic Broking Systems, banking system BS, the Internet INET, application office server RA, a certificate authority server CA, and a directory server DS.
[0030]Prepaid card PC is the noncontact IC card which stored the electronic value information about an electronic value beforehand. This prepaid card PC is provided with the function which transmits the stored electronic value information to an external node by radio, and functions as a user's electronic purse. According to this embodiment, infrared rays, such as IrDA (Infrared Data Association), are used, for example.
[0031]Moving machine MS is a portable telephone, for example, and performs voice communication and data communications via the mobile radio communication network MN. This moving machine MS builds in the IC card which manages the memory and input and output of electronic value information about an electronic value. Hereafter, this IC card is called UIM(User Identity Module)1. It becomes possible by equipping moving machine MS with this UIM1 to operate this moving machine MS of a user as an electronic purse. More specifically, moving machine MS realizes various kinds of commercial transactions by reading the electronic value information in UIM1, and exchanging this with an external node. The case where electronic value information is transmitted and received between the electronic bank servers Electronic Broking Systems via the mobile radio communication network MN as a gestalt which exchanges this electronic value, and the electronic value information transmitted by infrared rays from prepaid card PC may be received.
[0032]The mobile radio communication network MN consists of base station MBS or an exchange station which does not illustrate, and provides voice communication service and data transmission services to moving machine MS. This mobile radio communication network MN is connected to the Internet INET via the gateway unit which is not illustrated.
[0033]It is connected to the mobile radio communication network MN on the electronic bank server Electronic Broking Systems, and also is connected to banking system BS installed in the bank which is not illustrated by the dedicated line. On this electronic bank server Electronic Broking Systems, the virtual bank account (it is hereafter called an electronic account) assigned to each user is established. The electronic bank server Electronic Broking Systems has memorized the electronic account number for specifying an electronic account, the balance of the electronic value in an electronic account, etc., and processes a deposit of the electronic value in an electronic account, a cash drawer, transfer, etc. according to the demand from moving machine MS. The electronic bank server Electronic Broking Systems has also memorized the balance of the electronic value in an electronic purse called not only an electronic account but moving machine MS and prepaid card PC which were mentioned above, and updates the balance by notice from these electronic purses. Therefore, even if the electronic bank server Electronic Broking Systems is a case where an electronic value is unjustly rewritten, for example by the electronic purse side called moving machine MS and prepaid card PC, it can detect the unjust rewriting by comparing with the balance which self memorizes.

[0034]Certificate authority server CA is a server of the common knowledge which publishes the electronic certificate of X.standard 509 conformity based on a RSA public-key crypto system, and is connected to the Internet INET. Certificate authority server CA performs the electronic signature for guaranteeing the justification to the public key of each node according to the issuance request of the public key certification transmitted from each node on a network, and, specifically, draws up a public key certification. Since this electronic signature is performed by the secret key for a signature which certificate authority server CA holds, each node which acquired the public key certification decodes this public key certification by the public key of certificate authority server CA distributed beforehand. In order that each of above-mentioned nodes may encipher data and may transmit by the public key of certificate authority server CA to certificate authority server CA, certificate authority server CA has memorized the secret key for decoding for decoding this cryptogram.
[0035]Directory server DS is a server of the common knowledge which stores the cancellation list CRL (Certificate Revocation List) of the public key certification which certificate authority server CA drew up, and this public key certification, and is connected to the Internet INET. Out of the public key certification which self stores, this directory server DS searched the public key certification corresponding to the acquisition request of each node, and is provided with the function to distribute this. In this embodiment, the public key of moving machine MS and the electronic bank server Electronic Broking Systems, Since certificate authority server CA receives issue of a public key certification, the node used as the communications partner of moving machine MS or the electronic bank server Electronic Broking Systems, By acquiring a public key certification from directory server DS, and verifying an electronic title, it can check that there is no spoofing.
[0036]It is the server provided on the Internet INET, and application office server RA receives the establishment application of the electronic account by a user, it cooperates with the electronic bank server Electronic Broking Systems, certificate authority CA, and directory server DS, and performs processing about establishment of an electronic account. This application office server RA has memorized the secret key for a signature, and the certificate for the codes for certificate authorities. The secret key for a signature is a key for application office server RA to perform an electronic signature to the data which should be transmitted to an external node, and this prevents him from the 3rd person being set to application office server RA, and clearing up. The certificate for the codes for certificate authorities is a certificate of the public key for enciphering the data which should be transmitted to certificate authority server CA. The cryptogram by this certificate for the codes for certificate authorities is decoded with the secret key for decoding of certificate authority server CA. The 3rd person is prevented from intercepting by this the data transmitted to certificate authority server CA.
[0037](2) Explain the composition of the electronic bank server Electronic Broking Systems, referring to the block diagram shown in the composition, next drawing 2 of the electronic bank server Electronic Broking Systems. As shown in the figure, the electronic bank server Electronic Broking Systems comprises the communications department 11, the control section 12, the database 13, and the bus 14 that connects these mutually.
[0038]The communications department 11 consists of a connection interface (graphic display abbreviation) and a communication control circuit (graphic display abbreviation) with the Internet INET. This communications department 31 performs certificate authority server CA, directory server DS, and data communications via the mobile radio communication network MN and the Internet INET, and also performs moving machine MS and data communications via the mobile radio communication network MN.
[0039]The control section 12 comprises CPU (Central Processing Unit), ROM (Read Only Memory), and RAM (Random Access Memory) which are not illustrated, and controls this whole electronic bank server Electronic Broking Systems.
[0040]The database 13 memorizes the information (henceforth, electronic value management information) for managing the electronic value information stored in the electronic value information and prepaid card PC which are stored in moving machine MS besides the various keys for using for an electronic signature, or a code and decoding. Drawing 3 is a figure explaining the

data memorized by the database 13. As shown in the figure, "the secret key for a signature", "the secret key for decoding", "the certificate for certificate authority signature verification", and "electronic value management information" are memorized by the database 13. "The secret key for a signature" is a secret key for performing an electronic signature to the data which the electronic bank server Electronic Broking Systems transmits to an external node. The public key corresponding to this secret key for a signature is registered into directory server DS after a certificate is published by certificate authority server CA. "The secret key for decoding" is a secret key for decoding the cryptogram which the electronic bank server Electronic Broking Systems received. The public key corresponding to this secret key is registered into directory server DS after a certificate is published by certificate authority server CA. "The certificate for certificate authority signature verification" is a certificate of the public key for verifying the electronic signature which certificate authority server CA performed to various certificates with the secret key. Since this certificate for certificate authority signature verification is registered into directory server DS, the electronic bank server Electronic Broking Systems can acquire this by accessing directory server DS.

[0041]Next, the "electronic value management information" mentioned above is explained in detail, referring to drawing 4 and drawing 5. Drawing 4 is a figure explaining the electronic value management information for managing the electronic value information stored in UIM1 of moving machine MS. As shown in the figure, electronic value management information, "Electronic bank ID", an "electronic account number", "the amount of an electronic value of an electronic account", It consists of "the amount of an electronic value of UIM", "it being a time stamp at the time of renewal of the amount of an electronic value", "the amount of a current electronic value of an electronic account", "the amount of a current electronic value of UIM", "it being a time stamp at the time of renewal of the amount of a current electronic value", and an "electronic value update history." "Electronic bank ID" is the identification information of the electronic bank server Electronic Broking Systems which published the electronic value. An "electronic account number" is the identification information for specifying each electronic account. "The amount of an electronic value of an electronic account" is the balance of the electronic value in the electronic account at the time of finally moving machine MS accessing with the electronic bank server Electronic Broking Systems. "The amount of an electronic value of UIM" is the balance of the electronic value in UIM1 at the time of finally moving machine MS accessing with the electronic bank server Electronic Broking Systems. "It is a time stamp at the time of renewal of an electronic value" is information which shows the time by which "the amount of an electronic value of UIM" was updated, and it is published by the electronic bank server Electronic Broking Systems. By using this time stamp, as it mentions later, unjust resending of an electronic value can be discovered. "The amount of a current electronic value of an electronic account" is the balance of the present electronic value in an electronic account. "The amount of a current electronic value of UIM" is the balance of the electronic value which should be reflected in UIM1. When it has the notice of a transaction log from either among this moving machine, it has the electronic value which should be stored in both moving machine MSs according to this calculated, when this exchanges an electronic value, without passing the electronic bank server Electronic Broking Systems by moving machine MSs so that it may mention later, but. Under the present circumstances, the electronic value which should be reflected in UIM1 in moving machine MS of the side which is not communicating with the electronic bank server Electronic Broking Systems is equivalent to the amount of a current electronic value of this UIM. "It is a time stamp at the time of renewal of the amount of a current electronic value" is information which shows the time by which the amount of a current electronic value of an electronic account and the amount of a current electronic value of UIM were updated. By using this time stamp, as it mentions later, unjust resending of an electronic value can be discovered. An "electronic value update history" is information which will show the update history of "the amount of an electronic value of UIM" by the time it results now from the time of finally moving machine MS accessing with the electronic bank server Electronic Broking Systems.

[0042]Next, the electronic value management information for managing the electronic value information stored in prepaid card PC is explained, referring to drawing 5. The point that the

electronic value management information shown in the figure differs from the electronic value management information shown in drawing 4 is in the place which replaces with UIM1 and is setting prepaid card PC as the object as an electronic purse, and the place which replaces with an "electronic account number" and uses "prepaid card ID." Thus, in UIM1 and prepaid card PC, although the electronic value management information in the electronic bank server Electronic Broking Systems has a difference, this is based on the following reasons. That is, UIM1 and an electronic account are because it is made to correspond with an electronic account and is not managed to corresponding fixed by 1 to 1, since prepaid card PC is negotiable, but an electronic value is managed using ID of each prepaid card.

[0043](3) Explain the composition of moving machine MS, referring to the block diagram shown in the composition, next drawing 6 of moving machine MS. As shown in the figure, moving machine MS comprises the Radio Communications Department 2, the control section 3, the user interface 4, UIM1, the infrared ray communication section 5, and the bus 6 that connects these mutually.

[0044]The Radio Communications Department 2 consists of an antenna which is not illustrated or a communication control circuit, and performs base station MBS and radio of the mobile radio communication network MN. The infrared ray communication section 5 performs infrared ray communication between prepaid card PCs.[0045]The control section 3 comprises CPU, ROM, and RAM which are not illustrated, and controls this whole moving machine MS. Here, two kinds of modes of the "money mode" for performing processing about the "communicate mode" for performing voice communication and data communications and an electronic value can be set to moving machine MS. A control section controls each part of moving machine MS according to the setting condition in each of these modes. For example, in the case of money mode, the control section 2 processes electronic authentication, code and decoding, time stamp generation and verification, secret lock management, and public key certification management etc.

[0046]The user interface 4 consists of a microphone and a loudspeaker for the liquid crystal panel for displaying a keypad for a user to perform alter operation and a variety of information and a user to talk over the telephone.

[0047]Hereafter, the data memorized by UIM1 is explained, referring to drawing 7. As shown in the figure, "the secret key for a signature", "the secret key for decoding", "the certificate for electronic bank signature verification", "the certificate for the codes for electronic banks", "the certificate for certificate authority signature verification", "user ID", and "electronic value information" are memorized by UIM1. "The secret key for a signature" is a secret key for performing an electronic signature to the data which moving machine MS transmits to an external node. Thus, he is prevented from the 3rd person becoming a user of moving machine MS, and clearing up by performing an electronic signature to the data transmitted to an external node. "The secret key for decoding" is a secret key for decoding the cryptogram which moving machine MS received. Thus, since a cryptogram is transmitted to moving machine MS, the 3rd person's tapping can be prevented. "The certificate for electronic bank signature verification" is a certificate of the public key for verifying the electronic signature which the electronic bank server Electronic Broking Systems signed. That is, in order that the electronic bank server Electronic Broking Systems may perform an electronic signature to the data addressed to moving machine MS, he is prevented from the 3rd person becoming the electronic bank server Electronic Broking Systems, and clearing up. "The certificate for the codes for electronic banks" is a certificate of the public key for enciphering the data transmitted to the electronic bank server Electronic Broking Systems. That is, since it is enciphered, the data transmitted to the electronic bank server Electronic Broking Systems from moving machine MS can prevent the 3rd person's tapping. "The certificate for certificate authority signature verification" is a certificate of the public key for verifying the electronic signature which certificate authority server CA performed to various certificates. That is, the reliability of the certificate which certificate authority server CA published will be secured. "User ID" is the identification information for specifying the user of moving machine MS.

[0048]As shown in drawing 8, electronic value information Next, "electronic bank ID", It consists of "electronic purse classification", an "electronic account number", "electronic bank signature SGN1", "the amount of an electronic value of an electronic account", "the amount of an electronic value of UIM", "it being a time stamp at the time of renewal of the amount of an

electronic value", "electronic bank signature SGN2", "the amount of a current electronic value", and an "electronic value update history." "Electronic bank ID" is as stated above. "Electronic purse classification" is information which shows whether the electronic purse which stores electronic value information is UIM1, or it is prepaid card PC. An "electronic account number" is as stated above. "Electronic bank signature SGN1" is the electronic signature which the electronic bank server Electronic Broking Systems gave, in order to guarantee that there is no alteration in the above "electronic bank ID", "electronic purse classification", and an "electronic account number." "The amount of an electronic value of an electronic account" is the balance of the electronic value in the electronic account at the time of finally moving machine MS accessing with the electronic bank server Electronic Broking Systems. "The amount of an electronic value of UIM" is the balance of the electronic value in UIM1 at the time of finally moving machine MS accessing with the electronic bank server Electronic Broking Systems. "It is a time stamp at the time of renewal of the amount of an electronic value" is information which shows the time by which the amount of an electronic value in UIM1 was updated, and this is published by the electronic bank server Electronic Broking Systems. "Electronic bank ID", the "electronic purse classification", and the "electronic account number" which "electronic bank signature SGN2" mentioned above, In order to guarantee that "the amount of an electronic value of an electronic account", "the amount of an electronic value of UIM", and all of "being a time stamp at the time of renewal of the amount of an electronic value" are not altered, it is an electronic signature which the electronic bank server Electronic Broking Systems gives. "The amount of a current electronic value" is the balance of the electronic value which UIM1 has memorized now. An "electronic value update history" is information which will show the update history of "the amount of an electronic value of UIM" by the time it results now from the time of finally moving machine MS accessing with the electronic bank server Electronic Broking Systems.

[0049]Drawing 9 is a figure showing the detailed contents of the "electronic value update history." As shown in the figure, an "electronic value update history" consists of a "receiving area electronic account number", the "payment side electronic account number", "payment side prepaid card ID", "transaction money amount", and a "business-contacts electronic signature." A "receiving area electronic account number" is an "electronic account number" of the near user who received the electronic value at the time of dealings, and the "payment side electronic account number" is an "electronic account number" of the near user who paid the electronic value at the time of dealings. When the payment side of electronic money is prepaid card PC, "payment side prepaid card ID" is registered as an update history. "Transaction money amount" is a frame of the electronic value concerning dealings, and a "business-contacts electronic signature", In order to guarantee that there is no alteration in the above "receiving area electronic account number", the "payment side electronic account number", "payment side prepaid card ID", and "transaction money amount", it is the electronic signature which business contacts' moving machine MS performed. Moving machine MS transmits an "electronic value update history" which was mentioned above after dealings to the electronic bank server Electronic Broking Systems.

[0050](3) Composition of prepaid card PC Next, the data memorized by prepaid card PC is explained. As drawing 10 is shown in the figure which is a figure showing the data memorized by prepaid card PC, "the certificate for electronic bank signature verification", "the certificate for the codes for electronic banks", "the certificate for certificate authority signature verification", and "electronic value information" are memorized by prepaid card PC. Since "the certificate for electronic bank signature verification", "the certificate for the codes for electronic banks", and "the certificate for certificate authority signature verification" are information which is common in what UIM1 has memorized, they omit explanation. "The secret key for a signature" and "the secret key for decoding" which UIM1 has memorized are not memorized by prepaid card PC. Since this is accepted that a prepaid card is an owner in which the user who possesses prepaid card PC is just since it is negotiable unlike the case of moving machine MS, It is because it is not necessary to perform the electronic signature for preventing spoofing and it is not sent [data is enciphered and].

[0051]Next, the electronic value information in prepaid card PC is explained in detail, referring to drawing 11. As shown in the figure, electronic value information "Electronic bank ID", "electronic

purse classification", It consists of "prepaid card ID", "electronic bank signature SGN3", "the amount of an electronic value of a prepaid card", "it being a time stamp at the time of renewal of the amount of an electronic value", "electronic bank signature SGN4", "the amount of a current electronic value", and an "electronic value update history." Replace with UIM1 the point that the electronic value information in this prepaid card PC differs from the electronic value information in UIM1, and it is aimed at the electronic value in prepaid card PC, and also it is in the place which has not memorized "the amount of an electronic value of an electronic account." That is, since prepaid card PC is negotiable among users, it does not correspond fixed with a user's electronic account like UIM1 of moving machine MS. Therefore, prepaid card PC has not memorized the amount of the electronic value in an account. Since the "electronic value update history" shown in drawing 11 is information which is common in the "electronic value update history" in UIM1 shown in drawing 10 except for the point that the object of an electronic value is a thing in a prepaid card, it omits explanation. [0052]B: Explain operation, next operation of the embodiment which consists of the above-mentioned composition. Below, establishment of (1) electronic account, continuation of (2) electronic accounts, and (3) electronic values deposit - Pull out, it divides, without the exchange between (4) electronic purses, and transfer of (5) electronic values, and explanation of operation is given.
[0053](1) Establishment drawing 12 of an electronic account is a sequence diagram showing operation of the whole system in the case of establishing an electronic account. First, a user goes to the application office (graphic display abbreviation) in which application office server RA is installed, The account number of the bank account for appropriating an electronic value for the telephone number of information required in order to establish an electronic account, for example, a name, an address, a password, and moving machine MS, and an own electronic account, etc. are notified to an operator. An operator inputs these information into application office server RA.
[0054]Application office server RA transmits the inputted information to the electronic bank server Electronic Broking Systems, and requests establishment of an electronic account (arrow **).
[0055]The electronic bank server Electronic Broking Systems asks banking system BS the existence and solvency of a bank account of a user, and if these are checked, it will carry out temporary establishment of the electronic account (arrow **). At this time, an "electronic account number" is published and the term of validity of this electronic account is set up.
[0056]Subsequently, the electronic bank server Electronic Broking Systems transmits the term of validity of an "electronic account number" and an electronic account to application office server RA (arrow **).
[0057]Application office server RA will generate the key pair (namely, pair of a secret key and a public key) corresponding to a user according to this, if the term of validity of an "electronic account number" and an electronic account is received. There are two kinds of things of the electronic signature of the data which should be transmitted to the electronic bank server Electronic Broking Systems from moving machine MS, the key pair for that verification, and the key pair for the code and decoding of the data which should be transmitted to moving machine MS from the electronic bank server Electronic Broking Systems in this key pair. The term of validity of this key pair is the same as the term of validity of an electronic account number. And application office server RA sends the public key for performing the public key for verifying the electronic signature of the key pairs created with the "electronic account number", and encryption to certificate authority server CA, and requests publishing the public key certification to these keys (arrow **).
[0058]According to this, certificate authority server CA publishes the public key certification for electronic signature verification and for codes, relates these with an "electronic account number", and registers them into directory server DS (arrow **).
[0059]On the other hand, it is checked by the electronic bank server's Electronic Broking Systems accessing directory server DS, and using an "electronic account number" as a key and searching it that the public key certification for electronic signature verification and for codes has been registered (arrow **). This means having become possible to perform communication from which security was secured between the electronic bank server Electronic Broking Systems and moving machine MS.

[0060]And the electronic bank server Electronic Broking Systems specifies an "electronic account number", and notifies application office server RA that the electronic account which the number shows may be used (arrow **).
[0061]According to this, application office server RA accesses directory server DS, and acquires "the certificate for electronic bank signature verification", "the certificate for the codes for electronic banks", and "the certificate for certificate authority signature verification" which are beforehand stored there (arrow **).
[0062]And application office server RA writes in "the secret key for a signature", "the secret key for decoding", "the certificate for electronic bank signature verification", "the certificate for the codes for electronic banks", "the certificate for certificate authority signature verification", "electronic bank ID", and an "electronic account number" via the ROM writer which is not illustrated to UIM1. A user receives UIM1 in which these information was written, moving machine MS is equipped with this, and processing is ended (arrow **).
[0063](2) As it is the continuation **** of an electronic account, the user can establish an electronic account, but the continuous use of the electronic account established once becomes possible by paying account management charge periodically. The gestalt of the payment of this account management charge has the following. . Namely, pull down the electronic value of account management charge from the (A) user's electronic account. (B). Charge directly the amount of money of account management charge to a user's actual bank account. (C). Appropriate the part for an equivalent for account management charge among the re-purchase prices of UIM1. (D) There are five methods of appropriating the part for an equivalent for account management charge among the installation expenses of the new key of UIM1 among the public key certification issue cost of a key pair which appropriates the part for an equivalent for account management charge and which was re-created within (E) UIM1.
[0064]The key in UIM1 is periodically updated newly as above-mentioned. In the system using the key based on a public-key-encryption algorithm, this is based on the reason it is common to set the term of validity as a key and to update periodically, in order to secure the safety of a key. the method of this concrete updating -- (**) -- the re-purchase of UIM1, and (**) -- UIM1 in application office server RA, [rewrite and (re-writing)] (c) It newly generates within the on-line download to UIM1 in moving machine MS from certificate authority server CA, and (d) UIM1, and there are four methods of requesting issue of a public key certification on-line to certificate authority server CA.
[0065]In the method (above (A)) which pulls down an electronic value from an electronic account and pays account management charge here to the electronic bank server Electronic Broking Systems as an example of renewal of UIM1, It explains referring to the sequence shown in drawing 13 for the method (the above-mentioned (**)) with which moving machine MS downloads on-line the secret key of the new key pairs which certificate authority server CA generates hereafter.
[0066]The electronic bank server Electronic Broking Systems notifies the pulling-down date and the amount of account management charge a priori to the user who wishes continuous use of an electronic account. And if the date comes, the electronic bank server Electronic Broking Systems will pull down an electronic value from a user's electronic account as account management charge for the next term (Step S1).
[0067]Subsequently, to a user's "electronic account number", after performing an electronic signature, it enciphers, and the electronic bank server Electronic Broking Systems is notified to application office server CA, and the download permission of a secret key to a key pair recurrence line and a user and public key certification issue are requested (Step S2).
[0068]On the other hand, by decryption and electronic signature verification, after certificate authority server CA checks that the above-mentioned request is a thing from the right electronic bank server Electronic Broking Systems, it generates a key pair and publishes the certificate of the generated public key. The published public key certification is registered into directory server DS (Step S3).
[0069]The electronic bank server Electronic Broking Systems accesses directory server DS, A check of that a new public key certification has been published will report that account management charge was received and that the preparation which downloads a secret key was

completed to moving machine MS of the user who does continuous use (Step S5). (step S4)
[0070]If moving machine MS is received [the notice in which the preparation which downloads a secret key from the electronic bank server Electronic Broking Systems was completed], after displaying this notice, it requests download of a new secret key to certificate authority server CA according to a user's operation (Step S6).
[0071]If a request of download is received from moving machine MS, certificate authority server CA will encipher a new secret key by a user's old (it is effective now) public key for codes, will perform an electronic signature, and will transmit to moving machine MS (Step S7).
[0072]Moving machine MS verifies the electronic signature performed to the new secret key received from certificate authority server CA, and checks surely having been sent from right certificate authority server CA. The sent secret key is decrypted with effective "secret key for decoding" now (Step S8).
[0073]Subsequently, moving machine MS transposes the old secret key in UIM1 to a new secret key (step S9). And moving machine MS signs and transmits the message of a purport which succeeded in replacement of a secret key with new "secret key for a signature" to certificate authority server CA (Step S10).
[0074]On the other hand, certificate authority server CA will register the public key to an old secret key into CRL of directory server DS, if the message of a purport which succeeded in replacement of a secret key is received (Step S11). Thereby, the public key to an old secret key becomes unusable.
[0075](3) Explain a deposit and the operation to pay of the electronic value to UIM1 or prepaid card PC, referring to a deposit and the sequence which is paid, next is shown in drawing 14 and drawing 15 of an electronic value. Below, the case where pull out 100 of "amount of electronic value of electronic account" 1000 yen yen, and it appropriates for UIM1 is mentioned as an example, and is explained. First, whether does a user operate the keypad of moving machine MS and the electronic value in prepaid card PC is used. The amount of money (namely, transaction money amount) to deposit in whether the electronic value in UIM1 built in moving machine MS is used to the amount of money or an electronic account to choose and pull out from an electronic account further is inputted. Here, UIM1 is chosen as an electronic purse and the drawer amount of money of 100 yen is inputted. Moving machine MS receives the above-mentioned key operation (step Sa1).
[0076]Subsequently, moving machine MS receives the information inputted in step Sa1, and the electronic value information in UIM1, After enciphering using "the certificate for the codes for electronic banks" stored in UIM1, performing the electronic signature with "the secret key for a signature" and giving a time stamp further, it transmits to the electronic bank server Electronic Broking Systems by making this into a requirement signal (step Sa2).
[0077]If the above-mentioned requirement signal is received, the electronic bank server Electronic Broking Systems will use the "electronic account number" within the received electronic value information as a key, will acquire the public key certification for electronic signature verification from directory server DS, and will verify the justification of the electronic signature of moving machine MS using this (step Sa3).
[0078]Subsequently, the electronic bank server Electronic Broking Systems decodes the cryptogram received by step Sa2 using "the secret key for decoding" which self has memorized, and checks a time stamp further (step Sa4). With the check of this time stamp, it is the processing which checks that two or more requirement signals with which the same time stamp was given from the same user do not exist. The danger of unjust resending of a requirement signal can be prevented by this processing.
[0079]Subsequently, the electronic bank server Electronic Broking Systems checks and pulls out the specified drawer amount of money or the deposit amount of money, or calculates "the amount of an electronic value of UIM" after a deposit, and "the amount of an electronic value of an electronic account" (step Sa5). Here, "the amount of an electronic value of UIM" after a drawer changes to 100 yen, and "the amount of an electronic value of an electronic account" changes to 900 yen. [0080]Next, the electronic bank server Electronic Broking Systems uses an "electronic account number" as a key, and acquires the public key certification for codes from directory

server DS (step Sa6).
[0081]And a calculated value [in / in the electronic bank server Electronic Broking Systems / step Sa5] etc. It enciphers using the public key certification for codes acquired from directory server DS to the transaction kind and transaction money amount in which the exception of an "electronic account number", a user name, a drawer, or a deposit is shown (step Sa7).
[0082]To the above-mentioned cryptogram, after the electronic bank server Electronic Broking Systems performs an electronic signature using "the secret key for a signature" which self has memorized, it gives a time stamp and transmits to moving machine MS (step Sa8).
[0083]Moving machine MS performs verification of an electronic signature, decoding of a cryptogram, and the check of a time stamp to the received data (step Sa9).
[0084]Moving machine MS is pulled out or displays "the amount of an electronic value of UIM" and "the amount of an electronic value of an electronic account" after a deposit (step Sa10). Here, "the amount of an electronic value of UIM" changes to 100 yen, and "the amount of an electronic value of an electronic account" changes to 900 yen. A user inspects this visually and performs key operation of O.K. which shows whether they are an own demand and a thing to adjust, or NG.
[0085]When the key operation of O.K. is made here, moving machine MS updates the electronic value information memorized by UIM1 (step Sa11). Namely, after updating "the amount of an electronic value of the electronic account" shown in drawing 8 from 1000 yen to 900 yen, updating "the amount of an electronic value of UIM" from 0 yen to 100 yen and updating "the amount of a current electronic value" from 0 yen to 100 yen, The time stamp and electronic signature which were received are stored as "it is a time stamp at the time of renewal of the amount of an electronic value", and "electronic bank signature SGN2", respectively.
[0086]And moving machine MS creates the message which shows that the key operation of O.K. was made, and receives this message, After performing processing of encryption by "the certificate for the codes for electronic banks", the electronic signature by "the secret key for a signature", and time stamp grant like step Sa2, it transmits to the electronic bank server Electronic Broking Systems (step Sa12).
[0087]Next, in drawing 15, if the above-mentioned message is received, like step Sa3, the electronic bank server Electronic Broking Systems will acquire "the certificate for electronic signature verification" from directory server DS, and will verify the justification of an electronic signature using this (step Sa13). Like step Sa4, the electronic bank server Electronic Broking Systems decodes a cryptogram using "the secret key for decoding", and checks a time stamp (step Sa14).
[0088]As a result, the electronic bank server Electronic Broking Systems updates the electronic value management information shown in drawing 4, when the message which shows the purport of O.K. is checked (step Sa15). Here, "the amount of an electronic value of an electronic account" is updated from 1000 yen to 900 yen, After updating "the amount of an electronic value of UIM" from 0 yen to 100 yen, updating the amount of a current electronic value of the electronic account from 1000 yen to 900 yen and updating the amount of a current electronic value of UIM from 0 yen to 100 yen, The time stamp at this time is published and this is stored as "it being a time stamp at the time of renewal of the amount of an electronic value", and "being a time stamp at the time of renewal of the amount of a current electronic value."
[0089]And the electronic bank server Electronic Broking Systems transmits the message of the purport that dealings were completed to moving machine MS (step Sa16). On the other hand, moving machine MS displays the message which received (step Sa17), and processing is ended.
[0090]In the above-mentioned example, when the key operation in step Sa10 is NG, moving machine MS does not update the electronic value information in UIM1. And in step Sa12, the message which shows the purport of NG is created and it transmits to the electronic bank server Electronic Broking Systems. And in step Sa13, the electronic bank server Electronic Broking Systems will end processing, without updating electronic value management information, if the message of NG is received. However, the electronic bank server Electronic Broking Systems keeps the log concerning the above-mentioned processing with the electronic signature of moving machine MS. This is used in order to cope with a claim etc. which are referred to as "Having inputted O.K. as an identification result" from the user of moving machine MS later.

[0091]Now, when the above-mentioned processing is not completed for the reason of the electronic bank server Electronic Broking Systems being unable to receive the message from moving machine MS in step Sa12, for example, To the non completion message of the purport that dealings were not completed, and the amount of an electronic value in UIM1 before dealings, like step Sa8, the electronic bank server Electronic Broking Systems performs an electronic signature to moving machine MS, after enciphering, it gives a time stamp, and transmits to moving machine MS. On the other hand, when a non completion message is received from the electronic bank server Electronic Broking Systems, moving machine MS displays the message and transposes it to "the amount of an electronic value of UIM" before the dealings to which "the amount of an electronic value of UIM" has been sent with the non completion message.
[0092]When moving machine MS is not both able to receive a completion message or a non completion message, for example by communication interception over a long period of time, etc., moving machine MS displays the message which shows dealings the purport that it does not complete on an indicator. A user operates after restoration and moving machine MS from communication interception etc., does a communication interface to the electronic bank server Electronic Broking Systems, acquires the electronic value information after updating, and updates own electronic value information.
[0093]In the above-mentioned example, although the electronic value in UIM1 of moving machine MS was mentioned as the example and explained, when making a deposit [the electronic value in prepaid card PC / an electronic account], prepaid card PC should just perform the same processing as the above via moving machine MS by performing infrared ray communication.
[0094](4) Exchange moving machine MS between electronic purses can exchange an electronic value by the local means of communication which does not intervene the electronic bank server Electronic Broking Systems like infrared ray communication. Below, referring to the sequence shown in drawing 16 and drawing 17, a moving machine MS1 to 100 of user A yen electronic value is paid, the case where moving machine MS2 of the user B receives this is mentioned as an example, and explanation of operation is given.
[0095]First, according to the user's A key operation moving machine MS1, The requirement signal which requires "electronic bank signature SGN1" to "electronic bank ID" in the user's B electronic value information, "electronic purse classification", an "electronic account number", and these is transmitted with infrared rays to moving machine MS2 of the user B (step Sb1).
[0096]If this requirement signal is received, moving machine MS2 of the user B will read the electronic value information demanded from UIM1 of self, and it will transmit this to moving machine MS1 by infrared ray communication (step Sb2).
[0097]Moving machine MS1 verifies "electronic bank signature SGN1" in the received electronic value information, and the user B checks that he is a just owner of the electronic value which the electronic bank server Electronic Broking Systems publishes (step Sb3). Processing is ended when it cannot check.
[0098]Next, the user A performs key operation which directs payment, after inputting the "electronic purse classification" (here, referred to as UIM1) which pays an electronic value as the electronic value amount of money of 100 yen paid to the user B. Moving machine MS1 receives this key operation (step Sb4).
[0099]moving machine MS1 [subsequently,] -- the user's B "electronic account number", the user's A "electronic account number", and "transaction money amount" (here) The amount of electronic value 100 yen which moving machine MS2 is paid from moving machine MS1 is used as an information set, the user's A electronic signature is performed to this information set, and it transmits to moving machine MS2 as "electronic value information which the user A pays." Under the present circumstances, "electronic bank signature SGN1" to "electronic bank ID" of the user A in the electronic value information which self has memorized, "electronic purse classification", an "electronic account number", and these doubles and transmits moving machine MS1 (step Sb5).

[0100]Moving machine MS2 verifies "electronic bank signature SGN1" which received, and the user A checks that he is a just owner of the electronic value which the electronic bank server Electronic Broking Systems publishes (step Sb6). Processing is ended when it cannot check.

[0101]Moving machine MS2 verifies the user's A electronic signature performed to the received information set (step Sb7). It enables this to prevent the 3rd person from becoming and clearing up to moving machine MS1 of the user A.
[0102]Subsequently, moving machine MS2 displays the information except the user's A electronic signature among received "the electronic value information which A pays" (step Sb8). That is, the user's B "electronic account number", the user's A "electronic account number", and the "transaction money amount" of 100 yen will be displayed here. The user B will input into moving machine MS2 directions of the purport that it is O.K., if satisfactory with reference to this display. On the other hand, when there is a problem, the user B inputs into moving machine MS2 directions of the purport that it is NG. Moving machine MS2 notifies moving machine MS1 that it is NG, and it ends processing.
[0103]Next, moving machine MS2 receives "the amount of a current electronic value of UIM" in the electronic value information memorized in UIM1 of self, The amount of electronic value 100 yen equivalent to "transaction money amount" is added, and an update history is added to an "electronic value update history" based on "the electronic value information which A pays" received from moving machine MS1 (step Sb9).
[0104]Next, information excluding [moving machine MS2] the user's A electronic signature among "the electronic value information which A pays", That is, the user's B electronic signature is performed to the user's B "electronic account number", the user's A "electronic account number", and the "transaction money amount" of 100 yen, and this is transmitted to moving machine MS1 as "electronic value information which B received" (step Sb10).
[0105]Moving machine MS1 will verify the user's B electronic signature performed to this, if "the electronic value information which the user B received" is received (step Sb11).
[0106]Next, moving machine MS1 reduces the amount of electronic value 100 yen which is equivalent to "transaction money amount" from "the amount of a current electronic value of UIM" in the electronic value information memorized to UIM1 of self, Based on "the electronic value information which the user B received", an update history is added to an "electronic value update history" (step Sb12). At this time, the exchange of the local electronic value between moving machine MS1 and moving machine MS2 will be completed.
[0107]Next, after moving machine MS2 of the user B who received the payment of the electronic value ends the processing shown in drawing 16, the sequence shown in drawing 17 is started when it is necessary to communicate with the electronic bank server Electronic Broking Systems. First, it requests that moving machine MS2 reads an "electronic value update history", transmits this to the electronic bank server Electronic Broking Systems, and checks the justification of dealings from UIM1 of self (step Sc1).
[0108]On the other hand, an electronic bank server Electronic Broking Systems server verifies the user's A electronic signature the "business-contacts electronic signature" within this "electronic value update history", and here with reference to the "electronic value update history" received from moving machine MS2. If satisfactory as a result of this verification, the following electronic value management information will be changed (step Sc2). Concerning [namely,] the electronic value management information corresponding to the user B who is an electronic value receiving area, 100 yen is added to "the amount of an electronic value of UIM", it updates "it is a time stamp at the time of renewal of the amount of an electronic value", 100 yen is added to "the amount of a current electronic value of UIM", and processing which updates "it is a time stamp at the time of renewal of the amount of a current electronic value" is performed. About the electronic value management information corresponding to the user A who is a payment side of an electronic value, "the amount of a current electronic value of UIM" of 100 yen is reduced, and processing which updates "it is a time stamp at the time of renewal of the amount of a current electronic value" is performed. When there is a problem in the verification result of a "business-contacts electronic signature", the electronic bank server Electronic Broking Systems creates the message of the purport that it was not able to update since there was a problem, and notifies the administrator of the electronic bank server Electronic Broking Systems of it.
[0109]Now, the electronic bank server Electronic Broking Systems transmits the electronic value information which should be updated to moving machine MS2 based on the electronic value

management information updated in step Sc2 (step Sc3). The electronic value information transmitted here is "the amount of an electronic value of UIM", "it being a time stamp at the time of renewal of the amount of an electronic value", and "electronic bank signature SGN2." Here, when there is a problem in the verification result of a "business-contacts electronic signature" as mentioned above, the message of the purport that it was not able to update since there was a problem which was mentioned above is also doubled, and it transmits to moving machine MS2.

[0110]Moving machine MS2 updates the electronic value information in UIM1 according to the electronic value information received from the electronic bank server Electronic Broking Systems (step Sc4).

[0111]Now, when moving machine MS1 communicates with the electronic bank server Electronic Broking Systems in the processing generated behind like moving machine MS2, it receives the check of own electronic value information from the electronic bank server Electronic Broking Systems. That is, when the electronic bank server Electronic Broking Systems receives access from moving machine MS1, it compares "the amount of a current electronic value of UIM" with "the amount of an electronic value of UIM" among the "electronic value management information" corresponding to the user A. If it seems that both differ, electronic value management information will be updated. The contents of updating here are combining "the amount of an electronic value of UIM" with "the amount of a current electronic value of UIM", and updating "it being a time stamp at the time of renewal of the amount of an electronic value."

[0112]According to the contents of updating of electronic value management information mentioned above, the electronic bank server Electronic Broking Systems transmits the electronic value information which should be updated to moving machine MS1. That is, "the amount of an electronic value of UIM", "it being a time stamp at the time of renewal of the amount of an electronic value", and "electronic bank signature SGN2" are transmitted.

[0113]If moving machine MS1 verifies "electronic bank signature SGN2" among the electronic value information received from the electronic bank server Electronic Broking Systems and it is satisfactory, it will update the electronic value information in UIM1 (step Sb20). Payment processing will be guaranteed by the electronic bank server Electronic Broking Systems by the above processing, and it will complete.

[0114]Thus, the exchange between electronic purses is completed as effective processing only after an "electronic value update history" reaches the electronic bank server Electronic Broking Systems from the both sides of a dealings subject's electronic purse. However, it may be judged as a processing conclusion only by notifying the "electronic value update history" of not only this but one of electronic purses. In this case, processing can be completed also by notifying not the update history of the side which thought that the electronic value mentioned above but the update history of the side which paid the electronic value to the electronic bank server Electronic Broking Systems.

[0115]In the above-mentioned example, although it paid, and UIM1 of moving machine MS was mentioned as the example and it was explained as a near electronic purse, of course, it is also possible to use the electronic value in prepaid card PC. In this case, prepaid card PC should just perform the same processing as the above via moving machine MS by performing infrared ray communication.

[0116](5) The transfer electronic value of an electronic value is a form of the transfer to its electronic purse or electronic account to others' electronic account, and can be transferred to others. Transfer of an electronic value is explained referring to the sequence shown in drawing 18 hereafter.

[0117]First, a user chooses the drawer origin (henceforth, transfer origin) of the electronic value which operates and transfers moving machine MS. Although chosen from three, UIM1 in prepaid card PC and moving machine MS, and a user's own electronic account **, specifically, UIM1 should be chosen here. Subsequently, a user inputs an "electronic account number" (following and transfer place electronic account number) and the amount of money (amount of money for henceforth, transfer) to transfer of a transfer place. Moving machine MS receives the above alter operation (SUTETSUSd1).

[0118]Subsequently, moving machine MS gives a time stamp to the inputted information,

Encryption by the public key for the codes for electronic bank servers is performed, and the data which performed the electronic signature using "the secret key for a signature" is transmitted to the electronic bank server Electronic Broking Systems as a requirement signal which requires transfer (step Sd2). In step Sd1, when a user chooses prepaid card PC as an agency transferring money, moving machine MS performs prepaid card PC and infrared ray communication, and acquires the electronic value information in prepaid card PC, and this also transmits it to the electronic bank server Electronic Broking Systems simultaneously.

[0119]On the other hand, in the electronic bank server Electronic Broking Systems, it checks that there is no injustice by verification of an electronic signature, cryptogram decoding, and time stamp check to the received requirement signal (step Sd3).

[0120]Next, it checks payment of the specified transfer place electronic account being possible for the electronic bank server Electronic Broking Systems, or existing really in the state of establishment, and that it is more than the amount of transferred money as which the balance of the electronic value of the agency transferring money was specified (step Sd4). When prepaid card PC is chosen as an agency transferring money, the electronic bank server Electronic Broking Systems. By verifying "electronic bank signature SGN4", it is checked whether money can be transferred after checking that there is no unjust alteration to the amount of an electronic value of the agency (prepaid card PC) transferring money.

[0121]Next, the electronic bank server Electronic Broking Systems calculates the amount of an electronic value of the transfer origin (here UIM1) after transfer. And an "electronic bank ID" transfer place electronic account number, the user name of a transfer place electronic account, As opposed to the amount of money for transfer, the "electronic account number" of the user of the agency transferring money, and the amount of an electronic value of the transfer origin (UIM1) before and behind transfer, A time stamp is given, encryption by the public key for codes acquired from directory server DS is performed, an electronic signature is performed with "the secret key for a signature" which self memorizes, and it transmits to moving machine MS (step Sd5).

[0122]Moving machine MS checks that there is no injustice by electronic signature verification, cryptogram decoding, and time stamp check about the received data (step Sd6).

[0123]Subsequently, moving machine MS displays the received data. A user inspects this visually, and if alter operation which shows O.K. or NG is performed, moving machine MS will receive this (step Sd7). Here, when the alter operation which shows O.K. is made, the electronic value information which UIM1 [selected as an agency transferring money] has memorized is updated. Here, the electronic value information updated is "the amount of an electronic value of UIM", "it being a time stamp at the time of renewal of the amount of an electronic value", "electronic bank signature SGN2", and "the amount of a current electronic value." When an electronic account is chosen as an agency transferring money, the information in an electronic purse is not updated. When the alter operation which shows NG is made, the electronic value in an electronic purse is not updated.

[0124]Subsequently, moving machine MS creates the message which shows whether the received alter operation is O.K. or it is NG, To this message, time stamp grant, encryption by the public key for the codes for electronic banks, and the electronic signature by "the secret key for a signature" are performed, and it transmits to the electronic bank server Electronic Broking Systems (step Sd8).

[0125]When the electronic bank server Electronic Broking Systems receives the message of the purport of O.K., the amount of an electronic value in a transfer place electronic account is calculated, the electronic signature of the electronic bank server Electronic Broking Systems is performed, and this calculated value is stored as electronic value management information corresponding to the electronic account of the transferring destination (step Sd9). When an electronic account is chosen as an agency transferring money, the amount of an electronic value in a transferring money agency electronic account is calculated, and the electronic signature of the electronic bank server Electronic Broking Systems is performed to this calculated value, and it stores in it as electronic value management information.

[0126]The electronic bank server Electronic Broking Systems transmits the message of the purport that processing was completed to moving machine MS (step Sd10). Moving machine MS

displays the message which received and notifies a user of completion of a series of exchanges.
[0127]When the electronic bank server Electronic Broking Systems receives the message of the purport of NG, processing is ended without updating electronic value management information. However, the electronic bank server Electronic Broking Systems keeps the log concerning the above-mentioned processing with the electronic signature of moving machine MS. This is used in order to cope with a claim etc. which are referred to as "Having inputted O.K. as an identification result" from the user of moving machine MS later.
[0128]Now, when the above-mentioned processing is not completed for the reason of the electronic bank server Electronic Broking Systems being unable to receive the message from moving machine MS in step Sd8, for example, To the non completion message of the purport that dealings were not completed, and "the amount of an electronic value of UIM" before dealings, like step Sa8, the electronic bank server Electronic Broking Systems performs an electronic signature to moving machine MS, after enciphering, it gives a time stamp, and transmits to moving machine MS. On the other hand, when a non completion message is received from the electronic bank server Electronic Broking Systems, moving machine MS displays the message and transposes it to "the amount of an electronic value of UIM" before the dealings to which "the amount of an electronic value of UIM" has been sent with the non completion message.
[0129]When moving machine MS is not both able to receive a completion message or a non completion message, for example by communication interception over a long period of time, etc., moving machine MS displays the message which shows dealings the purport that it does not complete on an indicator. A user operates after restoration and moving machine MS from communication interception etc., does a communication interface to the electronic bank server Electronic Broking Systems, acquires the electronic value information after updating, and updates own electronic value information.
[0130]In the above-mentioned example, although the electronic value in UIM1 of moving machine MS was mentioned as the example and explained, when making a deposit [the electronic value in prepaid card PC], prepaid card PC should just perform the same processing as the above via moving machine MS by performing infrared ray communication.
[0131]C: Explain an application, next the application of an embodiment. For example, a vending machine and a POS (Point Of Sale) register are received, Incorporate the function of the electronic purse equivalent to UIM1 of moving machine MS, and between a customer's (namely, users, such as a vending machine) moving machine MS (or prepaid card PC), and a vending machine, Local communication can perform electronic value delivery between electronic purses, and goods can be sold with a cashless payment. In a vending machine, since the justification can be checked by verifying "electronic bank signature SGN1" when exchanging moving machine MS and an electronic value, it can be told to the electronic bank server Electronic Broking Systems each time that it is not necessary to check justification. Therefore, there is a merit that the purchase of goods can be performed promptly, for a customer, and there is a merit that communication charges with a server are pressed down for contractors, such as a vending machine.
[0132]It is also possible to sell goods with a cashless payment between a customer's moving machine MS, a vending machine, etc., without including the function of the electronic purse of moving machine MS in a vending machine. When exchanging moving machine MS and an electronic value also in this case, "electronic bank signature SGN1" is verified. This example is explained referring to drawing 19. vending machine server VS by which vending machine VM was connected to the mobile radio communication network -- a cable -- or wireless connection is carried out. The function which communicates by performing moving machine MS and infrared ray communication, the function to perform an electronic signature to the data transmitted to moving machine MS, and the function to verify "electronic bank signature SGN1" transmitted from moving machine MS are carried in vending machine VM.
[0133]Moving machine MS1 of a customer receives a vending machine contractor's "electronic account number" using the infrared ray communication between vending machine VM.
[0134]A customer inputs into moving machine MS the electronic value amount of money and the "electronic purse classification" which are paid to vending machine VM, ranks second and does

operation which shows payment indication. Moving machine MS receives this alter operation.
[0135]Moving machine MS makes a set a vending machine contractor's "electronic account number", a customer's "electronic account number", and amount information equivalent to the electronic value to pay, performs a customer's electronic signature to this, and transmits to vending machine VM by infrared ray communication as "electronic value information which a customer pays." The information set of "electronic bank signature SGN1" to "electronic bank server ID", "electronic purse classification", an "electronic account number", and these also transmits to vending machine VM simultaneously among the electronic value information stored in a customer's electronic purse.
[0136]Vending machine VM verifies "electronic bank signature SGN1" which received, and checks that a customer is an owner of the electronic value which the right electronic bank server Electronic Broking Systems published. Here, when the verification result of an electronic signature is NG, processing with a customer is stopped and logging of the received information is carried out as a thing with the possibility of unjust access.
[0137]When the above-mentioned electronic signature verification is O.K., vending machine VM checks that the amount information equivalent to the electronic value to pay is more than a merchandise sum. When this is insufficient, vending machine VM stops processing with moving machine MS, and replies the message of the purport that the amount of money is insufficient to moving machine MS.
[0138]When the above-mentioned amount-of-money check is O.K., logging of vending machine VM is carried out by making the electronic signature of the "electronic account number" of the vending machine contractor who received, a customer's "electronic account number", the amount information equivalent to the electronic value to pay, and a customer into an "electronic value update history." And vending machine VM performs an electronic signature to the message of the purport that the commodity price was received, and replies it to moving machine MS. At this time, the payment of the commodity price to vending machine VM is completed, in vending machine VM, it will be in the state where the depression of the button of commodity selection can be carried out, and delivery of goods will be completed.
[0139]And moving machine MS updates the electronic value information in UIM1 based on the message which received from vending machine VM. The information to update reduces the commodity price paid from "the amount of a current electronic value", It is adding the electronic signature of a vending machine contractor's "electronic account number", a customer's "electronic account number", the amount information equivalent to the electronic value to pay, and vending machine VM to an "electronic value update history."
[0140]The logging information of vending machine VM is periodically collected by vending machine server VS, and is sent to the electronic bank server Electronic Broking Systems.
[0141]In an electronic bank server Electronic Broking Systems server, to the "electronic value update history" received from vending machine server VS, it pays, a person's electronic signature is verified, and the following management information is changed. Namely, about the electronic value management information of a vending machine VM contractor's electronic account. Process an "amount of electronic value of electronic account" addition, and the renewal of "being a time stamp at the time of renewal of the amount of an electronic value" of an electronic account, and about the electronic value management information of the electronic account and electronic purse of a customer. The "amount of current electronic value" cut of UIM1 and renewal of "being a time stamp at the time of renewal of the amount of an electronic value" are processed. Here, when a customer pays with prepaid card PC, an "amount of current electronic value of prepaid card" cut and renewal of "being a time stamp at the time of renewal of the amount of an electronic value" are processed about prepaid card PC.
[0142]When there is a problem in an electronic authentication result, the electronic bank server Electronic Broking Systems creates the message of the purport that it was not able to update since there was a problem, and notifies the administrator of the electronic bank server Electronic Broking Systems of it.
[0143]The electronic bank server Electronic Broking Systems transmits the contents of updating which followed the electronic value management information of a vending machine VM contractor's

electronic account, i.e., an "amount of electronic value of electronic account" addition, and the contents of renewal of "being a time stamp at the time of renewal of the amount of an electronic value" of an electronic account to vending machine server VS. When there is a problem in an electronic authentication result, the message mentioned above is also doubled and it transmits to vending machine server VS.

[0144]Vending machine server VS notifies the administrator of vending machine server VS of this by displaying the message received from the electronic bank server Electronic Broking Systems etc. When an administrator is received [the message of the purport that it was not able to update since there was a problem], after checking the contents, when accepting as fraudulent practice, he does management of appealing to a legal means.

[0145]When the electronic value information in a customer's electronic purse accesses the electronic bank server Electronic Broking Systems behind, by the procedure of the exchange between the electronic purses mentioned above, and the same procedure, payment processing is guaranteed to the electronic bank server Electronic Broking Systems, and completes it.

[0146]When the "electronic value update history" received from the customer is lost by the system trouble of vending machine VM or a vending machine server, Compatibility with a current electronic value is guaranteed with the same method as the case where an "electronic value update history" is lost in the exchange between electronic purses.

[0147]Thus, since the electronic bank server Electronic Broking Systems manages the amount of an electronic value of the both sides of an electronic account and an electronic purse according to the embodiment, it is detectable that an electronic value is unjustly rewritten by the electronic purse side. The justification can be checked only between electronic purses, without asking each time the electronic bank server Electronic Broking Systems by verifying "electronic bank signature SGN1", when an electronic value is locally exchanged between electronic purses. Therefore, there is no possibility of making the traffic on a network increasing. Since the electronic bank server Electronic Broking Systems updates at least the electronic value management information which self has managed by the notice from one of electronic purses, its efficiency improves. Since a time stamp is given at the time of dealings, unjust resending can be prevented using this.

[0148]D: As modification previous statement, this invention is not limited to the embodiment mentioned above, but following various change is possible for it.

(1) Gestalt moving machine MS of moving machine MS should just be a personal digital assistant which contains a wireless communication function, It may be a personal computer or PDA (Personal Digital Assistants) etc. which connects with a portable telephone other than the portable telephone mentioned above, and performs data communications.

[0149](2) Although moving machine MS, prepaid card PC, and vending machine VS perform radio which used infrared rays of each other in the communication configuration embodiment of a moving machine, a prepaid card, and a vending machine, Although not only this but the mobile station 50 which may be a wire communication is generally provided with 16 core connector which outputs and inputs a serial signal, The prepaid card PC and vending machine VS side is also equipped with the same thing as this, and it may be made to perform data communications by carrying out cable connection of these connectors mutually.

[0150](3) In the installation mode embodiment of each server, the electronic bank server Electronic Broking Systems was installed on the mobile radio communication network MN, and, as for application office server RA, certificate authority server CA, and directory server DS, it was installed on the Internet INET. However, the setting position of not only this but each server may be on which network.

[0151](4) Although a user's ****** generates and he was trying for application office server RA to write in UIM1 in the generation embodiment of a key pair, don't restrict to this. For example, it creates by the plant of UIM1, and it may write in beforehand and may create with the key pair generation function mounted in UIM1. It may be a gestalt which requests key pair generation from an organization like certificate authority server CA, and downloads this.

[0152](5) Electronic purses, as for, UIM1 or prepaid card PC carried out the storage capacity above-mentioned, such as UIM1 and prepaid card PC, The obstacle may have occurred in the memory storage of the "electronic value update history" according to the case where no

"electronic value update histories" cannot be stored with the shortage of a storage capacity, or the system trouble. In such a case, it is assumed that an "electronic value update history" is lost. A part may be lost in the form where the "electronic value update history" which oneself paid is deleted by a malicious user. By the way, in an embodiment, if it pays and one of "electronic value update histories" is sent to the electronic bank server Electronic Broking Systems as for a side and receipt side, it pays and can update to a right electronic value value about both side and receipt side. However, when it pays and the "electronic value update history" of the both sides of the side and receipt side is lost, the electronic bank server Electronic Broking Systems cannot grasp the exchange of an electronic value. In this case, in the timing which each electronic purse accessed behind at the electronic bank server Electronic Broking Systems since the exchange itself was not performed, Processing which takes compatibility according to "the electronic value amount of money of an electronic purse" in which the electronic bank server Electronic Broking Systems manages "the amount of a current electronic value of UIM" in each electronic purse is performed. That is, the electronic value information by the side of an electronic purse is compulsorily adjusted to the electronic value information by the side of an electronic bank. Under such a premise, at the time of dealings using the electronic value after it, moving machine MS may eliminate an "electronic value update history" from the old order at the time of a trade date, if it detects having accumulated the quantity "electronic value update history" equivalent to the storage capacity of an electronic purse. If it detects having accumulated the quantity "electronic value update history" equivalent to the storage capacity of an electronic purse, it may be made for moving machine MS to transmit compulsorily the "electronic value update history" to the electronic bank server Electronic Broking Systems. Thereby, the electronic value information by the side of an electronic purse and the electronic value information by the side of an electronic bank are adjusted. Moving machine MS may not be made not to conduct dealings using an electronic value after it, if it detects having accumulated the quantity "electronic value update history" equivalent to the storage capacity of an electronic purse. And that is displayed on an indicator and it processes notifying a user etc.

[0153](6) The local means of communication between moving machine MS, means-of-communication moving machine MS between prepaid card PCs, and prepaid card PC may not necessarily be limited to the infrared ray communication mentioned above, and this may be a different wireless communication means (registered trademark), for example, Bluetooth. Of course, it is possible similarly about the means of communication between moving machine MS and vending machine VM to use wireless communication means other than infrared rays.

[0154]

[Effect of the Invention]As mentioned above, while memorizing the balance of the electronic value in an electronic account according to this invention, Since the balance of the electronic value stored in the communication terminal as an electronic purse is memorized and the balance of the electronic value in a communication terminal is updated according to the contents of dealings, unjust rewriting of the electronic value by the side of a communication terminal is detectable (claims 1 and 24).

[0155]When the 1st communication terminal and 2nd communication terminal transmit and receive an electronic value mutually, the balance of the electronic value stored in a communication terminal is updated by the transaction log provided from either at least among the 1st communication terminal or the 2nd communication terminal. That is, since either may be sufficient as the communication terminal which transmits a transaction log, efficiency will improve (claim 2).

[0156]When the 1st communication terminal and 2nd communication terminal transmit and receive an electronic value mutually, the 1st communication terminal, While the identification information of the issue subject who published this electronic value, and the issue subject concerned do electronic signature addition to the electronic value which transmits, the 2nd communication terminal checks the justification of the electronic value which received by verifying the identification information and the electronic signature of the issue subject who received. Thereby, the justification of an electronic value will be checked only between communication terminals, and security can be secured efficiently (claims 9 and 20).

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－344537
（P2001－344537A）
(43)公開日　平成13年12月14日(2001.12.14)

(51)Int.Cl.⁷	識別記号	ＦＩ	テーマコード（参考）
Ｇ０６Ｆ　17/60	４１０	Ｇ０６Ｆ　17/60	４１０Ｃ　５Ｂ０４９
	４２０		４２０　５Ｂ０５５
	４３２		４３２Ａ
	５０６		５０６

審査請求　未請求　請求項の数26　ＯＬ　（全 23 頁）

(21)出願番号　特願2000－163676(P2000－163676)

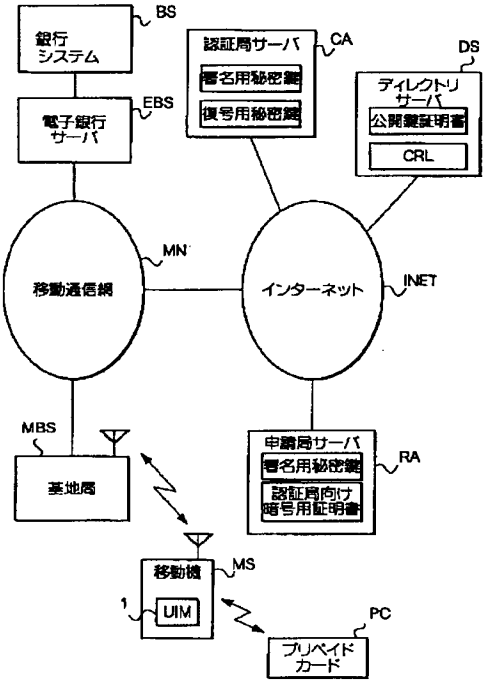
(22)出願日　平成12年５月31日(2000.5.31)

(71)出願人　392026693
株式会社エヌ・ティ・ティ・ドコモ
東京都千代田区永田町二丁目11番１号
(72)発明者　木下　眞希
東京都千代田区永田町二丁目11番１号　株式会社エヌ・ティ・ティ・ドコモ内
(72)発明者　山下　哲也
東京都千代田区永田町二丁目11番１号　株式会社エヌ・ティ・ティ・ドコモ内
(74)代理人　100098084
弁理士　川▲崎▼　研二　（外２名）

Ｆターム(参考)　5B049 AA05 BB46 EE21 GG03 GG06
5B055 BB04 CB01 EE13 EE27 FA01
HB06 LL07

(54)【発明の名称】　電子バリューシステム、通信端末及びサーバ

(57)【要約】
【課題】　セキュリティを確保するとともに、効率性を向上させる電子バリューシステムを提供する。
【解決手段】　電子銀行サーバＥＢＳは、電子口座内の電子バリュー額とともに、移動機ＭＳ内のＵＩＭ１に格納された電子バリュー額を記憶しており、電子バリューを用いた取引の内容に応じて、これを更新する。



FP03-0308
JP
'08.5.07
OA

【特許請求の範囲】

【請求項１】　電子的な金銭情報である電子バリューを管理する電子バリューシステムであって、

ネットワーク上のサーバに設けられ、複数のユーザのそれぞれに割り当てられた電子口座毎に前記電子バリューを蓄積する電子口座保持手段と、

前記電子バリューを格納するメモリと、外部ノードとの間で前記電子バリューを送受信する通信手段とを有し、前記ユーザの電子財布として用いられる複数の通信端末と、

前記電子口座保持手段から前記ネットワークを介して、前記通信端末のメモリに前記電子バリューをダウンロードするダウンロード手段と、

前記ネットワーク上に設けられ、前記通信端末のメモリに格納される電子バリューの残高情報を記憶、更新する財布残金管理手段と、

前記通信端末から前記財布残金管理手段に対し、前記ネットワークを介して、前記電子バリューを用いた取引の内容を示す取引ログを通知する取引ログ通知手段とを備え、

前記財布残金管理手段は、前記通知される取引ログに基づいて前記電子バリューの残高情報を記憶、更新することを特徴とする電子バリューシステム。

【請求項２】　請求項１に記載の電子バリューシステムにおいて、

前記複数の通信端末は、前記電子バリューを互いに送受信する第１の通信端末及び第２の通信端末を含み、

前記第１の通信端末の通信手段は、前記メモリに格納されている電子バリューとともに自己の識別情報を前記第２の通信端末に送信し、

前記第２の通信端末の通信手段は、前記第１の通信端末から送信された電子バリュー及び前記第１の通信端末の識別情報を受信する一方、自己の識別情報を前記第１の通信端末に送信し、

前記取引ログ通知手段は、第１の通信端末又は前記第２の通信端末のうち少なくともいずれか一方から前記財布残金管理手段に対し、前記送受信された電子バリューの額と、前記第１の通信端末及び前記第２の通信端末の識別情報とを前記取引ログとして送信し、

前記財布残金管理手段は、前記送信されてくる取引ログに基づいて、前記電子バリューの残高情報を更新することを特徴とする電子バリューシステム。

【請求項３】　請求項２に記載の電子バリューシステムにおいて、

前記第１の通信端末及び前記第２の通信端末は、自身の取引にかかる前記取引ログを蓄積するログ蓄積手段を有し、

前記第１の通信端末又は前記第２の通信端末のうち少なくともいずれか一方は、前記ログ蓄積手段による記憶容量に相当する前記取引ログを蓄積すると、外部ノードと電子バリューの送受信を行わないことを特徴とする電子バリューシステム。

【請求項４】　請求項２に記載の電子バリューシステムにおいて、

前記第１の通信端末及び前記第２の通信端末は、自身の取引にかかる前記取引ログを蓄積するログ蓄積手段を有し、

前記第１の通信端末又は前記第２の通信端末のうち少なくともいずれか一方は、前記ログ蓄積手段による記憶容量に相当する前記取引ログを蓄積すると、それ以後の取引時においては取引日時の古い順から前記取引ログを消去することを特徴とする電子バリューシステム。

【請求項５】　請求項２に記載の電子バリューシステムにおいて、

前記第１の通信端末及び前記第２の通信端末は、自身の取引にかかる前記取引ログを蓄積するログ蓄積手段を有し、

前記取引ログ通知手段は、前記第１の通信端末又は前記第２の通信端末のうち少なくともいずれか一方において前記ログ蓄積手段による記憶容量に相当する前記取引ログを蓄積すると、当該取引ログを前記財布残金管理手段に送信することを特徴とする電子バリューシステム。

【請求項６】　請求項１に記載の電子バリューシステムにおいて、

前記通信端末は、移動通信網に収容される移動通信端末であり、

前記ネットワークは、前記移動通信網であることを特徴とする電子バリューシステム。

【請求項７】　請求項２～５のいずれかに記載の電子バリューシステムにおいて、

前記通信端末は、移動通信網に収容される移動通信端末であり、

前記ネットワークは、前記移動通信網であり、

前記第１の通信端末の通信手段及び第２の通信端末の通信手段は、無線により通信を行うことを特徴とする電子バリューシステム。

【請求項８】　請求項１に記載の電子バリューシステムにおいて、

前記通信端末は、移動通信網に収容される移動通信端末であり、

前記通信端末のメモリは、当該通信端末に装着して使用されるＩＣカードであることを特徴とする電子バリューシステム。

【請求項９】　第１の通信端末及び第２の通信端末との間で、電子的な金銭情報である電子バリューを送受信する電子バリューシステムであって、

前記第１の通信端末は、

前記電子バリューと、当該電子バリューを発行した発行主体の識別情報と、当該識別情報に対し前記発行主体によって施された電子署名とを格納するメモリと、

前記格納されている電子バリューとともに、前記発行主体の識別情報及び電子署名を前記第２の通信端末に送信するための送信手段とを備え、
前記第２の通信端末は、
前記第１の通信端末から送信された電子バリューとともに、前記発行主体の識別情報及び電子署名とを受信する受信手段と、
前記受信した電子署名を検証することにより、前記第１の通信端末から送信されてきた電子バリューが前記発行主体により発行されたことを確認し、これにより、前記第１の通信端末の正当性を判断する判断手段とを備えることを特徴とする電子バリューシステム。
【請求項１０】　請求項９に記載の電子バリューシステムにおいて、
前記第２の通信端末は、
前記電子バリューと、当該電子バリューを発行した発行主体の識別情報と、当該識別情報に対し前記発行主体によって施された電子署名とを格納するメモリと、
前記格納されている前記発行主体の識別情報及び電子署名を前記第１の通信端末に送信するための送信手段とを備え、
前記第１の通信端末は、
前記第２の通信端末に対し前記電子バリューを送信する前に、前記第２の通信端末のメモリ内の前記発行主体の識別情報と当該識別情報に対し前記発行主体によって施された電子署名とを取得する取得手段と、
前記取得した電子署名を検証することにより、前記第２の通信端末のメモリ内の電子バリューは前記発行主体により発行されたことを確認し、これにより、前記第２の通信端末の正当性を判断する判断手段とを備えることを特徴とする電子バリューシステム。
【請求項１１】　請求項９又は１０に記載の電子バリューシステムにおいて、
前記第１の通信端末及び前記第２の通信端末は、自身の取引にかかる前記取引ログを蓄積するログ蓄積手段を有し、
前記第１の通信端末又は前記第２の通信端末のうち少なくともいずれか一方は、前記ログ蓄積手段による記憶容量に相当する前記取引ログを蓄積すると、自身が記憶している電子バリューの残高情報を管理している外部ノードに対し、前記蓄積した取引ログを送信することを特徴とする電子バリューシステム。
【請求項１２】　請求項９～１１のいずれかに記載の電子バリューシステムにおいて、
前記第１の通信端末及び前記第２の通信端末は、無線により電子バリューの送受信を行うことを特徴とする電子バリューシステム。
【請求項１３】　請求項９～１２のいずれかに記載の電子バリューシステムにおいて、
前記第１の通信端末又は前記第２の通信端末の少なくともいずれか一方は、移動通信網に収容される移動通信端末であることを特徴とする電子バリューシステム。
【請求項１４】　請求項９～１３のいずれかに記載の電子バリューシステムにおいて、
前記第２の通信端末は、商品を販売する自動販売機に内蔵されていることを特徴とする電子バリューシステム。
【請求項１５】　請求項１～１４のいずれかに記載の電子バリューシステムにおいて、
前記通信端末は、前記電子バリューを外部に送信する際には、その送信日時を当該電子バリューに付加して送信することを特徴とする電子バリューシステム。
【請求項１６】　請求項１～１５に記載の電子バリューシステムにおいて、
前記通信端末は、
外部と前記電子バリューを送受信する際に、当該電子バリューに対し鍵を用いて電子認証及び暗号・復号の処理を行うセキュリティ手段と、
前記鍵を定期的に更新する更新手段とを備えることを特徴とする電子バリューシステム。
【請求項１７】　電子的な金銭情報である電子バリュー及び自己の識別情報を格納するメモリと、
外部ノードとの間で前記電子バリューの送受信を行う通信手段と、
前記メモリに格納されている自己の識別情報を前記外部ノードに与える一方、前記外部ノードから当該外部ノードの識別情報を取得する識別情報交換手段と、
前記外部ノードとの間で送受信された前記電子バリューの額と、前記自己の識別情報及び前記外部ノードの識別情報とを取引ログとして蓄積するログ蓄積手段とを備え、前記ログ蓄積手段による記憶容量に相当する前記取引ログを蓄積すると、前記外部ノードとの間で前記電子バリューの送受信を行わないことを特徴とする通信端末。
【請求項１８】　電子的な金銭情報である電子バリュー及び自己の識別情報を格納するメモリと、
外部ノードとの間で前記電子バリューの送受信を行う通信手段と、
前記メモリに格納されている自己の識別情報を前記外部ノードに与える一方、前記外部ノードから当該外部ノードの識別情報を取得する識別情報交換手段と、
前記外部ノードとの間で送受信された前記電子バリューの額と、前記自己の識別情報及び前記外部ノードの識別情報とを、送受信日時とともに取引ログとして蓄積するログ蓄積手段とを備え、前記ログ蓄積手段による記憶容量に相当する前記取引ログを蓄積すると、それ以後の前記電子バリューの送受信時においては、前記蓄積されている取引ログを送受信日時の古い順から消去することを特徴とする通信端末。
【請求項１９】　電子的な金銭情報である電子バリュー及び自己の識別情報を格納するメモリと、

外部ノードとの間で前記電子バリューの送受信を行う通信手段と、
前記メモリに格納されている自己の識別情報を前記外部ノードに与える一方、前記外部ノードから当該外部ノードの識別情報を取得する識別情報交換手段と、
前記外部ノードとの間で送受信された前記電子バリューの額と、前記自己の識別情報及び前記外部ノードの識別情報とを、送受信日時とともに取引ログとして蓄積するログ蓄積手段とを備え、前記ログ蓄積手段による記憶容量に相当する前記取引ログを蓄積すると、前記蓄積されている取引ログを、当該取引ログを用いて前記電子バリューの送受信についての正当性を確認する外部装置に送信することを特徴とする通信端末。
【請求項２０】　電子的な金銭情報である電子バリューと、当該電子バリューの発行主体の識別情報と、当該識別情報に対し前記発行主体によって施された電子署名とを格納するメモリと、
外部ノードとの間で前記電子バリューの送受信を行う通信手段と、
前記通信手段によって前記外部ノードに送信される電子バリューに対し、前記発行主体の識別情報及び前記電子署名を付加する付加手段と、
前記通信手段によって前記外部ノードから受信した電子バリューに付加された前記発行主体の識別情報及び前記電子署名を検証することにより、前記電子バリューの正当性を確認する確認手段とを備えることを特徴とする通信端末。
【請求項２１】　請求項１７～２０に記載の通信端末において、
前記通信端末は、
外部と前記電子バリューを送受信する際に、当該電子バリューに対し鍵を用いて電子認証及び暗号・復号の処理を行うセキュリティ手段と、
前記鍵を定期的に更新する更新手段とを備えることを特徴とする通信端末。
【請求項２２】　請求項１７～２１のいずれかに記載の通信端末において、
前記電子バリューを前記外部ノードに送信する際に、その送信日時を前記電子バリューに付加して送信することを特徴とする通信端末。
【請求項２３】　請求項１７～２２のいずれかに記載の通信端末において、
前記通信手段は、無線により前記外部ノードとの間で前記電子バリューの送受信を行うことを特徴とする通信端末。
【請求項２４】　請求項１７～２３のいずれかに記載の通信端末において、
前記通信端末は、移動通信網に収容される移動通信端末であり、
前記メモリは、当該通信端末に装着して使用されるＩＣカードであることを特徴とする通信端末。
【請求項２５】　電子的な金銭情報である電子バリューを記憶するサーバであって、
ユーザに割り当てられた電子口座毎に前記電子バリューを蓄積する電子口座保持手段と、
前記電子バリューを格納するメモリと、外部ノードとの間で前記電子バリューを送受信する通信手段とを有した通信端末に対し、前記電子口座保持手段によって蓄積されている電子バリューを前記ネットワークを介してダウンロードするダウンロード手段と、
前記通信端末のメモリに格納される電子バリューの残高情報を記憶する財布残金記憶手段と、
前記通信端末における前記電子バリューを用いた取引の内容を示す取引ログを、前記通信端末から前記ネットワークを介して取得するログ取得手段と、
前記取得した取引ログに基づいて、前記財布残金記憶手段により記憶されている前記電子バリューの残高情報を更新する財布残金更新手段と、
を備えることを特徴とするサーバ。
【請求項２６】　請求項２５に記載のサーバであって、
前記ダウンロードされる電子バリュー情報に対し、自身が記憶する鍵により電子認証を施す電子認証手段を備えることを特徴とするサーバ。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、電子バリューを用いて電子商取引を行うための電子バリューシステム、通信端末及びサーバに関する。
【０００２】
【従来の技術】電子的な金銭情報（以下、電子バリューと呼ぶ）を用いて、キャッシュレスショッピングを行うためのシステムが各種提案されている。
【０００３】
【発明が解決しようとする課題】ところで、この電子バリューは単なるデータにすぎないため、データそのものの改ざんや、電子バリューの所有者になりすますなどの不正が発生する虞があり、これを防止するためのセキュリティ確保が課題となっている。一方、セキュリティ確保のためのシステムを動作させるということは、そのための処理が増大することをも意味しており、システム全体の処理効率を劣化させる要因となる。本発明は、このような背景に鑑みてなされたものであり、セキュリティを確保するとともに、処理効率を向上させる電子バリューシステム、通信端末及びサーバを提供することを目的とする。
【０００４】
【課題を解決するための手段】上述した課題を解決するため、　請求項１に記載の発明は、電子的な金銭情報である電子バリューを管理する電子バリューシステムであって、ネットワーク上のサーバに設けられ、複数のユー

ザのそれぞれに割り当てられた電子口座毎に前記電子バリューを蓄積する電子口座保持手段と、前記電子バリューを格納するメモリと、外部ノードとの間で前記電子バリューを送受信する通信手段とを有し、前記ユーザの電子財布として用いられる複数の通信端末と、前記電子口座保持手段から前記ネットワークを介して、前記通信端末のメモリに前記電子バリューをダウンロードするダウンロード手段と、前記ネットワーク上に設けられ、前記通信端末のメモリに格納される電子バリューの残高情報を記憶、更新する財布残金管理手段と、前記通信端末から前記財布残金管理手段に対し、前記ネットワークを介して、前記電子バリューを用いた取引の内容を示す取引ログを通知する取引ログ通知手段とを備え、前記財布残金管理手段は、前記通知される取引ログに基づいて前記電子バリューの残高情報を記憶、更新することを特徴とする。

【０００５】請求項２に記載の発明は、請求項１に記載の電子バリューシステムにおいて、前記複数の通信端末は、前記電子バリューを互いに送受信する第１の通信端末及び第２の通信端末を含み、前記第１の通信端末の通信手段は、前記メモリに格納されている電子バリューとともに自己の識別情報を前記第２の通信端末に送信し、前記第２の通信端末の通信手段は、前記第１の通信端末から送信された電子バリュー及び前記第１の通信端末の識別情報を受信する一方、自己の識別情報を前記第１の通信端末に送信し、前記取引ログ通知手段は、第１の通信端末又は前記第２の通信端末のうち少なくともいずれか一方から前記財布残金管理手段に対し、前記送受信された電子バリューの額と、前記第１の通信端末及び前記第２の通信端末の識別情報とを前記取引ログとして送信し、前記財布残金管理手段は、前記送信されてくる取引ログに基づいて、前記電子バリューの残高情報を更新することを特徴とする。

【０００６】請求項３に記載の発明は、請求項２に記載の電子バリューシステムにおいて、前記第１の通信端末及び前記第２の通信端末は、自身の取引にかかる前記取引ログを蓄積するログ蓄積手段を有し、前記第１の通信端末又は前記第２の通信端末のうち少なくともいずれか一方は、前記ログ蓄積手段による記憶容量に相当する前記取引ログを蓄積すると、外部ノードと電子バリューの送受信を行わないことを特徴とする。

【０００７】請求項４に記載の発明は、請求項２に記載の電子バリューシステムにおいて、前記第１の通信端末及び前記第２の通信端末は、自身の取引にかかる前記取引ログを蓄積するログ蓄積手段を有し、前記第１の通信端末又は前記第２の通信端末のうち少なくともいずれか一方は、前記ログ蓄積手段による記憶容量に相当する前記取引ログを蓄積すると、それ以後の取引時においては取引日時の古い順から前記取引ログを消去することを特徴とする。

【０００８】請求項５に記載の発明は、請求項２に記載の電子バリューシステムにおいて、前記第１の通信端末及び前記第２の通信端末は、自身の取引にかかる前記取引ログを蓄積するログ蓄積手段を有し、前記取引ログ通知手段は、前記第１の通信端末又は前記第２の通信端末のうち少なくともいずれか一方において前記ログ蓄積手段による記憶容量に相当する前記取引ログを蓄積すると、当該取引ログを前記財布残金管理手段に送信することを特徴とする。

【０００９】請求項６に記載の発明は、請求項１に記載の電子バリューシステムにおいて、前記通信端末は、移動通信網に収容される移動通信端末であり、前記ネットワークは、前記移動通信網であることを特徴とする。

【００１０】請求項７に記載の発明は、請求項２～５のいずれかに記載の電子バリューシステムにおいて、前記通信端末は、移動通信網に収容される移動通信端末であり、前記ネットワークは、前記移動通信網であり、前記第１の通信端末の通信手段及び第２の通信端末の通信手段は、無線により通信を行うことを特徴とする。

【００１１】請求項８に記載の発明は、請求項１に記載の電子バリューシステムにおいて、前記通信端末は、移動通信網に収容される移動通信端末であり、前記通信端末のメモリは、当該通信端末に装着して使用されるＩＣカードであることを特徴とする。

【００１２】請求項９に記載の発明は、第１の通信端末及び第２の通信端末との間で、電子的な金銭情報である電子バリューを送受信する電子バリューシステムであって、前記第１の通信端末は、前記電子バリューと、当該電子バリューを発行した発行主体の識別情報と、当該識別情報に対し前記発行主体によって施された電子署名とを格納するメモリと、前記格納されている電子バリューとともに、前記発行主体の識別情報及び電子署名を前記第２の通信端末に送信するための送信手段とを備え、前記第２の通信端末は、前記第１の通信端末から送信された電子バリューとともに、前記発行主体の識別情報及び電子署名とを受信する受信手段と、前記受信した電子署名を検証することにより、前記第１の通信端末から送信されてきた電子バリューが前記発行主体により発行されたことを確認し、これにより、前記第１の通信端末の正当性を判断する判断手段とを備えることを特徴とする。

【００１３】請求項１０記載の発明は、請求項９に記載の電子バリューシステムにおいて、前記第２の通信端末は、前記電子バリューと、当該電子バリューを発行した発行主体の識別情報と、当該識別情報に対し前記発行主体によって施された電子署名とを格納するメモリと、前記格納されている前記発行主体の識別情報及び電子署名を前記第１の通信端末に送信するための送信手段とを備え、前記第１の通信端末は、前記第２の通信端末に対し前記電子バリューを送信する前に、前記第２の通信端末のメモリ内の前記発行主体の識別情報と当該識別情報に

対し前記発行主体によって施された電子署名とを取得する取得手段と、前記取得した電子署名を検証することにより、前記第２の通信端末のメモリ内の電子バリューは前記発行主体により発行されたことを確認し、これにより、前記第２の通信端末の正当性を判断する判断手段とを備えることを特徴とする。

【００１４】請求項１１記載の発明は、請求項９又は１０に記載の電子バリューシステムにおいて、前記第１の通信端末及び前記第２の通信端末は、自身の取引にかかる前記取引ログを蓄積するログ蓄積手段を有し、前記第１の通信端末又は前記第２の通信端末のうち少なくともいずれか一方は、前記ログ蓄積手段による記憶容量に相当する前記取引ログを蓄積すると、自身が記憶している電子バリューの残高情報を管理している外部ノードに対し、前記蓄積した取引ログを送信することを特徴とする。

【００１５】請求項１２記載の発明は、請求項９～１１のいずれかに記載の電子バリューシステムにおいて、前記第１の通信端末及び前記第２の通信端末は、無線により電子バリューの送受信を行うことを特徴とする。

【００１６】請求項１３記載の発明は、請求項９～１２のいずれかに記載の電子バリューシステムにおいて、前記第１の通信端末又は前記第２の通信端末の少なくともいずれか一方は、移動通信網に収容される移動通信端末であることを特徴とする。

【００１７】請求項１４記載の発明は、請求項９～１３のいずれかに記載の電子バリューシステムにおいて、前記第２の通信端末は、商品を販売する自動販売機に内蔵されていることを特徴とする。

【００１８】請求項１５に記載の発明は、請求項１～１４のいずれかに記載の電子バリューシステムにおいて、前記通信端末は、前記電子バリューを外部に送信する際には、その送信日時を当該電子バリューに付加して送信することを特徴とする。

【００１９】請求項１６に記載の発明は、請求項１～１５に記載の電子バリューシステムにおいて、前記通信端末は、外部と前記電子バリューを送受信する際に、当該電子バリューに対し鍵を用いて電子認証及び暗号・復号の処理を行うセキュリティ手段と、前記鍵を定期的に更新する更新手段とを備えることを特徴とする電子バリューシステム。

【００２０】請求項１７記載の発明は、電子的な金銭情報である電子バリュー及び自己の識別情報を格納するメモリと、外部ノードとの間で前記電子バリューの送受信を行う通信手段と、前記メモリに格納されている自己の識別情報を前記外部ノードに与える一方、前記外部ノードから当該外部ノードの識別情報を取得する識別情報交換手段と、前記外部ノードとの間で送受信された前記電子バリューの額と、前記自己の識別情報及び前記外部ノードの識別情報とを取引ログとして蓄積するログ蓄積手段とを備え、前記ログ蓄積手段による記憶容量に相当する前記取引ログを蓄積すると、前記外部ノードとの間で前記電子バリューの送受信を行わないことを特徴とする。

【００２１】請求項１８記載の発明は、電子的な金銭情報である電子バリュー及び自己の識別情報を格納するメモリと、外部ノードとの間で前記電子バリューの送受信を行う通信手段と、前記メモリに格納されている自己の識別情報を前記外部ノードに与える一方、前記外部ノードから当該外部ノードの識別情報を取得する識別情報交換手段と、前記外部ノードとの間で送受信された前記電子バリューの額と、前記自己の識別情報及び前記外部ノードの識別情報とを、送受信日時とともに取引ログとして蓄積するログ蓄積手段とを備え、前記ログ蓄積手段による記憶容量に相当する前記取引ログを蓄積すると、それ以後の前記電子バリューの送受信時においては、前記蓄積されている取引ログを送受信日時の古い順から消去することを特徴とする。

【００２２】請求項１９記載の発明は、電子的な金銭情報である電子バリュー及び自己の識別情報を格納するメモリと、外部ノードとの間で前記電子バリューの送受信を行う通信手段と、前記メモリに格納されている自己の識別情報を前記外部ノードに与える一方、前記外部ノードから当該外部ノードの識別情報を取得する識別情報交換手段と、前記外部ノードとの間で送受信された前記電子バリューの額と、前記自己の識別情報及び前記外部ノードの識別情報とを、送受信日時とともに取引ログとして蓄積するログ蓄積手段とを備え、前記ログ蓄積手段による記憶容量に相当する前記取引ログを蓄積すると、前記蓄積されている取引ログを、当該取引ログを用いて前記電子バリューの送受信についての正当性を確認する外部装置に送信することを特徴とする。

【００２３】請求項２０に記載の発明は、電子的な金銭情報である電子バリューと、当該電子バリューの発行主体の識別情報と、当該識別情報に対し前記発行主体によって施された電子署名とを格納するメモリと、外部ノードとの間で前記電子バリューの送受信を行う通信手段と、前記通信手段によって前記外部ノードに送信される電子バリューに対し、前記発行主体の識別情報及び前記電子署名を付加する付加手段と、前記通信手段によって前記外部ノードから受信した電子バリューに付加された前記発行主体の識別情報及び前記電子署名を検証することにより、前記電子バリューの正当性を確認する確認手段とを備えることを特徴とする。

【００２４】請求項２１に記載の発明は、請求項１７～２０に記載の通信端末において、前記通信端末は、外部と前記電子バリューを送受信する際に、当該電子バリューに対し鍵を用いて電子認証及び暗号・復号の処理を行うセキュリティ手段と、前記鍵を定期的に更新する更新手段とを備えることを特徴とする　請求項２１に記載の

発明は、請求項１７～２０のいずれかに記載の通信端末において、前記電子バリューを前記外部ノードに送信する際に、その送信日時を前記電子バリューに付加して送信することを特徴とする。

【００２５】請求項２３記載の発明は、請求項１７～２２のいずれかに記載の通信端末において、前記通信手段は、無線により前記外部ノードとの間で前記電子バリューの送受信を行うことを特徴とする

【００２６】請求項２４に記載の発明は、請求項１７～２３のいずれかに記載の通信端末において、前記通信端末は、移動通信網に収容される移動通信端末であり、前記メモリは、当該通信端末に装着して使用されるＩＣカードであることを特徴とする。

【００２７】請求項２５に記載の発明は、電子的な金銭情報である電子バリューを記憶するサーバであって、ユーザに割り当てられた電子口座毎に前記電子バリューを蓄積する電子口座保持手段と、前記電子バリューを格納するメモリと、外部ノードとの間で前記電子バリューを送受信する通信手段とを有した通信端末に対し、前記電子口座保持手段によって蓄積されている電子バリューを前記ネットワークを介してダウンロードするダウンロード手段と、前記通信端末のメモリに格納される電子バリューの残高情報を記憶する財布残金記憶手段と、前記通信端末における前記電子バリューを用いた取引の内容を示す取引ログを、前記通信端末から前記ネットワークを介して取得するログ取得手段と、前記取得した取引ログに基づいて、前記財布残金記憶手段により記憶されている前記電子バリューの残高情報を更新する財布残金更新手段と、を備えることを特徴とする。請求項２６に記載の発明は、請求項２５に記載のサーバであって、前記ダウンロードされる電子バリュー情報に対し、自身が記憶する鍵により電子認証を施す電子認証手段を備えることを特徴とする。

【００２８】

【発明の実施の形態】以下、図面を参照しながら、本発明の実施の形態について説明する。この実施形態では、ネットワーク上に設けられた電子銀行に各ユーザの電子口座を開設するとともに、各ユーザが所持する移動機を電子財布として利用する。この電子バリューのやり取りにおいては、ＰＫＩ（Public Key Infrastructure）ベースのＲＳＡ公開鍵暗号方式に基づく電子認証や暗号・復号の機能を活用することとする。

【００２９】Ａ：構成

まず、実施形態の構成について説明する。図１は、実施形態にかかるシステム全体の構成を示すブロック図である。同図に示すように、このシステムは、移動機ＭＳ、移動通信網ＭＮ、プリペイドカードＰＣ、電子銀行サーバＥＢＳ、銀行システムＢＳ、インターネットＩＮＥＴ、申請局サーバＲＡ、認証局サーバＣＡ、ディレクトリサーバＤＳから構成される。

【００３０】プリペイドカードＰＣは、電子バリューに関する電子バリュー情報を予め格納した非接触ＩＣカードである。このプリペイドカードＰＣは、格納している電子バリュー情報を無線により外部ノードに送信する機能を備えており、ユーザの電子財布として機能するものである。この実施形態では、例えばＩｒＤＡ（Infrared Data Association）等の赤外線を用いる。

【００３１】移動機ＭＳは、例えば携帯電話機であり、移動通信網ＭＮを介して音声通信やデータ通信を行う。この移動機ＭＳは、電子バリューに関する電子バリュー情報の記憶及び入出力を司るＩＣカードを内蔵する。以下、このＩＣカードをＵＩＭ（User Identity Module）１と呼ぶ。ユーザは、このＵＩＭ１を移動機ＭＳに装着することにより、この移動機ＭＳを電子財布として動作させることが可能となる。より具体的には、移動機ＭＳは、ＵＩＭ１内の電子バリュー情報を読み出し、これを外部ノードとやり取りすることにより、各種の商取引を実現する。この電子バリューをやり取りする形態としては、移動通信網ＭＮを介して電子銀行サーバＥＢＳとの間で電子バリュー情報を送受信する場合と、プリペイドカードＰＣから赤外線によって送信された電子バリュー情報を受信する場合とがある。

【００３２】移動通信網ＭＮは、基地局ＭＢＳや図示せぬ交換局からなり、移動機ＭＳに対し音声通信サービスやデータ通信サービスを提供する。この移動通信網ＭＮは、図示せぬゲートウェイ装置を介してインターネットＩＮＥＴに接続されている。

【００３３】電子銀行サーバＥＢＳ上には、移動通信網ＭＮに接続されるほか、図示せぬ銀行内に設置された銀行システムＢＳに専用線により接続されている。この電子銀行サーバＥＢＳ上には、各ユーザに割り当てられた仮想的な銀行口座（以下、電子口座と呼ぶ）が開設されている。電子銀行サーバＥＢＳは、電子口座を特定するための電子口座番号や電子口座内の電子バリューの残高等を記憶しており、移動機ＭＳからの要求に応じて電子口座における電子バリューの預け入れ、引出し、振込み等の処理を行うようになっている。また、電子銀行サーバＥＢＳは、上述した電子口座だけではなく、移動機ＭＳやプリペイドカードＰＣといった電子財布内の電子バリューの残高をも記憶しており、これら電子財布から通知により、その残高を更新するようになっている。従って、電子銀行サーバＥＢＳは、例えば移動機ＭＳやプリペイドカードＰＣという電子財布側で電子バリューが不正に書き換えられた場合であっても、自身が記憶する残高と比較することにより、その不正書き換えを検出することができるようになっている。

【００３４】認証局サーバＣＡは、ＲＳＡ公開鍵暗号方式に基づく、規格Ｘ．５０９準拠の電子証明書を発行する周知のサーバであり、インターネットＩＮＥＴに接続されている。具体的には、認証局サーバＣＡは、ネット

ワーク上の各ノードから送信されてくる公開鍵証明書の発行依頼に応じて、各ノードの公開鍵に対し、その正当性を保証するための電子署名を施して公開鍵証明書を作成する。この電子署名は認証局サーバＣＡが保持する署名用秘密鍵によって行われるため、公開鍵証明書を取得した各ノードは、予め配布される認証局サーバＣＡの公開鍵によってこの公開鍵証明書を復号するようになっている。また、上記の各ノードは認証局サーバＣＡに対し、認証局サーバＣＡの公開鍵でデータを暗号化して送信してくるため、認証局サーバＣＡは、この暗号文を復号するための復号用秘密鍵を記憶している。

【００３５】ディレクトリサーバＤＳは、認証局サーバＣＡが作成した公開鍵証明書や、この公開鍵証明書の無効化リストＣＲＬ（Certificate Revocation List）を格納する周知のサーバであり、インターネットＩＮＥＴに接続されている。このディレクトリサーバＤＳは、自身が格納している公開鍵証明書の中から、各ノードの取得要求に対応した公開鍵証明書を検索し、これを配布する機能を備えている。この実施形態においては、移動機ＭＳ及び電子銀行サーバＥＢＳの公開鍵は、認証局サーバＣＡにより公開鍵証明書の発行を受けるようになっているので、移動機ＭＳや電子銀行サーバＥＢＳの通信相手となるノードは、ディレクトリサーバＤＳから公開鍵証明書を取得して電子書名を検証することにより、なりすましがないことを確認することができる。

【００３６】申請局サーバＲＡは、インターネットＩＮＥＴ上に設けられたサーバであり、ユーザによる電子口座の開設申請を受け付け、電子銀行サーバＥＢＳ、認証局ＣＡ及びディレクトリサーバＤＳと連携して電子口座の開設に関する処理を実行する。この申請局サーバＲＡは、署名用秘密鍵と、認証局向け暗号用証明書とを記憶している。署名用秘密鍵とは、申請局サーバＲＡが外部ノードに送信すべきデータに対し電子署名を施すための鍵であり、これにより、第３者が申請局サーバＲＡになりすますことを防止する。また、認証局向け暗号用証明書とは、認証局サーバＣＡに送信すべきデータを暗号化するための公開鍵の証明書である。この認証局向け暗号用証明書による暗号文は、認証局サーバＣＡの復号用秘密鍵によって復号される。これにより、認証局サーバＣＡに送信するデータを第３者が盗聴することを防止する。

【００３７】（２）電子銀行サーバＥＢＳの構成

次に、図２に示すブロック図を参照しながら、電子銀行サーバＥＢＳの構成について説明する。同図に示すように、電子銀行サーバＥＢＳは、通信部１１、制御部１２、データベース１３、及びこれらを相互に接続するバス１４から構成される。

【００３８】通信部１１は、インターネットＩＮＥＴとの接続インタフェース（図示略）や通信制御回路（図示略）からなる。この通信部３１は、移動通信網ＭＮ及びインターネットＩＮＥＴを介して認証局サーバＣＡ、ディレクトリサーバＤＳとデータ通信を行うほか、移動通信網ＭＮを介して移動機ＭＳとデータ通信を行う。

【００３９】制御部１２は、図示せぬＣＰＵ（Central Processing Unit）、ＲＯＭ（Read Only Memory）、ＲＡＭ（Random Access Memory）から構成され、この電子銀行サーバＥＢＳ全体を制御する。

【００４０】データベース１３は、電子署名や暗号・復号に用いるための各種鍵のほか、移動機ＭＳに格納される電子バリュー情報及びプリペイドカードＰＣに格納される電子バリュー情報を管理するための情報（以下、電子バリュー管理情報）を記憶する。図３は、データベース１３に記憶されるデータを説明する図である。同図に示すように、データベース１３には、「署名用秘密鍵」、「復号用秘密鍵」、「認証局署名検証用証明書」、及び「電子バリュー管理情報」が記憶されている。「署名用秘密鍵」は、電子銀行サーバＥＢＳが外部ノードに対して送信するデータに電子署名を施すための秘密鍵である。この署名用秘密鍵に対応する公開鍵は、認証局サーバＣＡによって証明書が発行された後にディレクトリサーバＤＳに登録される。「復号用秘密鍵」は、電子銀行サーバＥＢＳが受信した暗号文を復号するための秘密鍵である。この秘密鍵に対応する公開鍵は、認証局サーバＣＡによって証明書が発行された後にディレクトリサーバＤＳに登録される。「認証局署名検証用証明書」は、認証局サーバＣＡが秘密鍵により各種証明書に施した電子署名を検証するための公開鍵の証明書である。この認証局署名検証用証明書はディレクトリサーバＤＳに登録されているので、電子銀行サーバＥＢＳはディレクトリサーバＤＳにアクセスすることにより、これを取得することができる。

【００４１】次に、上述した「電子バリュー管理情報」について、図４及び図５を参照しながら詳細に説明する。図４は、移動機ＭＳのＵＩＭ１に格納される電子バリュー情報を管理するための電子バリュー管理情報を説明する図である。同図に示すように、電子バリュー管理情報は、「電子銀行ＩＤ」、「電子口座番号」、「電子口座の電子バリュー額」、「ＵＩＭの電子バリュー額」、「電子バリュー額更新時タイムスタンプ」、「電子口座のカレント電子バリュー額」、「ＵＩＭのカレント電子バリュー額」、「カレント電子バリュー額更新時タイムスタンプ」、「電子バリュー更新履歴」からなる。「電子銀行ＩＤ」は、電子バリューを発行した電子銀行サーバＥＢＳの識別情報である。「電子口座番号」は、各電子口座を特定するための識別情報である。「電子口座の電子バリュー額」は、移動機ＭＳが最後に電子銀行サーバＥＢＳとアクセスした時点における、電子口座内の電子バリューの残高である。「ＵＩＭの電子バリュー額」は、移動機ＭＳが最後に電子銀行サーバＥＢＳとアクセスした時点における、ＵＩＭ１内の電子バリュ

一の残高である。「電子バリュー更新時タイムスタンプ」は、「ＵＩＭの電子バリュー額」が更新された日時を示す情報であり、電子銀行サーバＥＢＳによって発行される。このタイムスタンプを用いることにより、後述するようにして電子バリューの不正再送を発見することができる。「電子口座のカレント電子バリュー額」は、電子口座内の現在の電子バリューの残高である。「ＵＩＭのカレント電子バリュー額」は、ＵＩＭ１に反映すべき電子バリューの残高である。これは、後述するように、移動機ＭＳどうしで電子銀行サーバＥＢＳを介さずに電子バリューをやり取りした場合、この移動機のうちいずれか一方から取引ログの通知があると、これに応じて双方の移動機ＭＳに格納されているべき電子バリューを計算されるが、この際、電子銀行サーバＥＢＳと通信を行っていない側の移動機ＭＳ内のＵＩＭ１に反映すべき電子バリューが、このＵＩＭのカレント電子バリュー額に相当する。「カレント電子バリュー額更新時タイムスタンプ」は、電子口座のカレント電子バリュー額及びＵＩＭのカレント電子バリュー額が更新された日時を示す情報である。このタイムスタンプを用いることにより、後述するようにして電子バリューの不正再送を発見することができる。「電子バリュー更新履歴」は、移動機ＭＳが最後に電子銀行サーバＥＢＳとアクセスした時点から現在に至るまでに、「ＵＩＭの電子バリュー額」の更新履歴を示す情報である。

【００４２】次に、図５を参照しながら、プリペイドカードＰＣに格納される電子バリュー情報を管理するための電子バリュー管理情報について説明する。同図に示す電子バリュー管理情報が、図４に示す電子バリュー管理情報と異なる点は、ＵＩＭ１に代えてプリペイドカードＰＣを電子財布としての対象としているところと、「電子口座番号」に代えて「プリペイドカードＩＤ」を用いているところにある。このように、ＵＩＭ１とプリペイドカードＰＣでは、電子銀行サーバＥＢＳにおける電子バリュー管理情報に違いがあるが、これは以下の理由による。即ち、ＵＩＭ１と電子口座とは１対１で固定的に対応しているのに対し、プリペイドカードＰＣは譲渡可能であることから、電子口座と対応させて管理するのではなく、個々のプリペイドカードのＩＤを用いて電子バリューを管理するからである。

【００４３】（３）移動機ＭＳの構成

次に、図６に示すブロック図を参照しながら、移動機ＭＳの構成について説明する。同図に示すように、移動機ＭＳは、無線通信部２、制御部３、ユーザインタフェース４、ＵＩＭ１、赤外線通信部５、及びこれらを相互に接続するバス６から構成される。

【００４４】無線通信部２は、図示せぬアンテナや通信制御回路からなり、移動通信網ＭＮの基地局ＭＢＳと無線通信を行う。また、赤外線通信部５は、プリペイドカードＰＣとの間で赤外線通信を行う

【００４５】制御部３は、図示せぬＣＰＵ、ＲＯＭ、ＲＡＭから構成され、この移動機ＭＳ全体を制御する。ここで、移動機ＭＳには、音声通信やデータ通信を行うための「通信モード」と、電子バリューに関する処理を行うための「マネーモード」という２種類のモードが設定可能である。制御部は、これらの各モードの設定状況に応じて、移動機ＭＳの各部を制御する。例えば、マネーモードの場合、制御部２は、電子認証、暗号・復号、タイムスタンプ生成・検証、秘密鍵管理、公開鍵証明書管理等の処理を行うようになっている。

【００４６】ユーザインタフェース４は、ユーザが入力操作を行うためのキーパッド、各種情報を表示するための液晶パネル、ユーザが通話を行うためのマイクロホン及びスピーカからなる。

【００４７】以下、図７を参照しながら、ＵＩＭ１に記憶されるデータについて説明する。同図に示すように、ＵＩＭ１には、「署名用秘密鍵」、「復号用秘密鍵」、「電子銀行署名検証用証明書」、「電子銀行向け暗号用証明書」、「認証局署名検証用証明書」、「ユーザＩＤ」及び「電子バリュー情報」が記憶されている。「署名用秘密鍵」は、移動機ＭＳが外部ノードに対して送信するデータに電子署名を施すための秘密鍵である。このように、外部ノードに対して送信するデータに電子署名を施すことにより、第３者が移動機ＭＳのユーザになりすますことが防止される。「復号用秘密鍵」は、移動機ＭＳが受信した暗号文を復号するための秘密鍵である。このように、移動機ＭＳに対しては暗号文が送信されてくるため、第３者の盗聴を防止することができる。「電子銀行署名検証用証明書」は、電子銀行サーバＥＢＳが署名した電子署名を検証するための公開鍵の証明書である。即ち、電子銀行サーバＥＢＳは、移動機ＭＳ宛のデータに電子署名を施すため、第３者が電子銀行サーバＥＢＳになりすますことが防止される。「電子銀行向け暗号用証明書」は、電子銀行サーバＥＢＳに対して送信するデータを暗号化するための公開鍵の証明書である。即ち、移動機ＭＳから電子銀行サーバＥＢＳに送信されるデータは暗号化されるため、第３者の盗聴を防止することができる。「認証局署名検証用証明書」は、認証局サーバＣＡが各種証明書に施した電子署名を検証するための公開鍵の証明書である。即ち、認証局サーバＣＡが発行した証明書の信頼性が確保されることになる。「ユーザＩＤ」は、移動機ＭＳのユーザを特定するための識別情報である。

【００４８】次に、電子バリュー情報は、図８に示すように、「電子銀行ＩＤ」、「電子財布種別」、「電子口座番号」、「電子銀行署名ＳＧＮ１」、「電子口座の電子バリュー額」、「ＵＩＭの電子バリュー額」、「電子バリュー額更新時タイムスタンプ」、「電子銀行署名ＳＧＮ２」、「カレント電子バリュー額」、「電子バリュー更新履歴」からなる。「電子銀行ＩＤ」は、既述のと

おりである。「電子財布種別」は、電子バリュー情報を格納する電子財布が、ＵＩＭ１であるかプリペイドカードＰＣであるかということを示す情報である。「電子口座番号」は、既述のとおりである。「電子銀行署名ＳＧＮ１」は、上記「電子銀行ＩＤ」、「電子財布種別」及び「電子口座番号」に改ざんがないことを保証するために電子銀行サーバＥＢＳが付与した電子署名である。「電子口座の電子バリュー額」は、移動機ＭＳが最後に電子銀行サーバＥＢＳとアクセスした時点における、電子口座内の電子バリューの残高である。「ＵＩＭの電子バリュー額」は、移動機ＭＳが最後に電子銀行サーバＥＢＳとアクセスした時点における、ＵＩＭ１内の電子バリューの残高である。「電子バリュー額更新時タイムスタンプ」は、ＵＩＭ１内の電子バリュー額が更新された日時を示す情報であり、これは電子銀行サーバＥＢＳによって発行される。「電子銀行署名ＳＧＮ２」は、上述した「電子銀行ＩＤ」、「電子財布種別」及び「電子口座番号」、「電子口座の電子バリュー額」、「ＵＩＭの電子バリュー額」、及び「電子バリュー額更新時タイムスタンプ」の全てが改ざんされていないことを保証するために電子銀行サーバＥＢＳが付与する電子署名である。「カレント電子バリュー額」は、ＵＩＭ１が現在記憶している電子バリューの残高である。「電子バリュー更新履歴」は、移動機ＭＳが最後に電子銀行サーバＥＢＳとアクセスした時点から現在に至るまでに、「ＵＩＭの電子バリュー額」の更新履歴を示す情報である。

【００４９】図９は、「電子バリュー更新履歴」の詳細な内容を示す図である。同図に示すように、「電子バリュー更新履歴」は、「受取側電子口座番号」、「支払側電子口座番号」、「支払側プリペイドカードＩＤ」、「取引金額」、及び「取引相手電子署名」からなる。「受取側電子口座番号」は、取引時に電子バリューを受け取った側のユーザの「電子口座番号」であり、「支払側電子口座番号」は、取引時に電子バリューを支払った側のユーザの「電子口座番号」である。また、電子マネーの支払側がプリペイドカードＰＣであった場合、「支払側プリペイドカードＩＤ」が更新履歴として登録される。「取引金額」は、取引にかかる電子バリューの額であり、「取引相手電子署名」は、上記「受取側電子口座番号」、「支払側電子口座番号」、「支払側プリペイドカードＩＤ」、「取引金額」に改ざんがないことを保証するために取引相手の移動機ＭＳが施した電子署名である。移動機ＭＳは、取引後において、上述したような「電子バリュー更新履歴」を電子銀行サーバＥＢＳに送信するようになっている。

【００５０】（３）プリペイドカードＰＣの構成

次に、プリペイドカードＰＣに記憶されるデータについて説明する。図１０は、プリペイドカードＰＣに記憶されるデータを示す図である、同図に示すように、プリペイドカードＰＣには、「電子銀行署名検証用証明書」、「電子銀行向け暗号用証明書」、「認証局署名検証用証明書」、及び「電子バリュー情報」が記憶されている。「電子銀行署名検証用証明書」、「電子銀行向け暗号用証明書」及び「認証局署名検証用証明書」は、ＵＩＭ１が記憶しているものと共通する情報であるので説明を省略する。また、プリペイドカードＰＣには、ＵＩＭ１が記憶している「署名用秘密鍵」及び「復号用秘密鍵」は記憶されていない。これは、移動機ＭＳの場合とは異なり、プリペイドカードは譲渡可能であることから、プリペイドカードＰＣを所持しているユーザが正当な所有者であると認められるので、なりすましを防止するための電子署名を行う必要もないし、データが暗号化されて送られてくることもないからである。

【００５１】次に、図１１を参照しながら、プリペイドカードＰＣ内の電子バリュー情報について詳細に説明する。同図に示すように、電子バリュー情報は、「電子銀行ＩＤ」、「電子財布種別」、「プリペイドカードＩＤ」、「電子銀行署名ＳＧＮ３」、「プリペイドカードの電子バリュー額」、「電子バリュー額更新時タイムスタンプ」、「電子銀行署名ＳＧＮ４」、「カレント電子バリュー額」、「電子バリュー更新履歴」からなる。このプリペイドカードＰＣ内の電子バリュー情報がＵＩＭ１内の電子バリュー情報と異なる点は、ＵＩＭ１に代えてプリペイドカードＰＣ内の電子バリューを対象としているほか、「電子口座の電子バリュー額」を記憶していないところにある。即ち、プリペイドカードＰＣは、ユーザ間で譲渡可能であるため、移動機ＭＳのＵＩＭ１のようにユーザの電子口座と固定的に対応するものではない。したがって、プリペイドカードＰＣは、口座内電子バリュー額を記憶していないのである。また、図１１に示す「電子バリュー更新履歴」は、電子バリューの対象がプリペイドカード内のものである点を除いて、図１０に示すＵＩＭ１内の「電子バリュー更新履歴」と共通する情報であるので、説明を省略する

【００５２】Ｂ：動作

次に、上記構成からなる実施形態の動作について説明する。以下では、（１）電子口座の開設、（２）電子口座の継続、（３）電子バリューの預け入れ・引出し、（４）電子財布間のやり取り、（５）電子バリューの振込み、に分けて動作説明を行う。

【００５３】（１）電子口座の開設

図１２は、電子口座を開設する場合のシステム全体の動作を示すシーケンス図である。まず、ユーザは、申請局サーバＲＡが設置されている申請局（図示略）に出向き、電子口座を開設するために必要な情報、例えば、氏名、住所、パスワード、移動機ＭＳの電話番号、自身の電子口座に電子バリューを充当する為の銀行口座の口座番号等をオペレータに通知する。オペレータは、これらの情報を申請局サーバＲＡに入力する。

【００５４】申請局サーバＲＡは、入力された情報を電

子銀行サーバＥＢＳに送信し、電子口座の開設を依頼する（矢印①）。

【００５５】電子銀行サーバＥＢＳは、ユーザの銀行口座の有無や支払い能力を銀行システムＢＳに問い合わせて、これらが確認されると電子口座を仮開設する（矢印②）。この時点で、「電子口座番号」が発行され、この電子口座の有効期限が設定される。

【００５６】次いで、電子銀行サーバＥＢＳは、「電子口座番号」及び電子口座の有効期限を申請局サーバＲＡに送信する（矢印③）。

【００５７】申請局サーバＲＡは、「電子口座番号」及び電子口座の有効期限を受信すると、これに応じて、ユーザに対応した鍵対（即ち、秘密鍵と公開鍵のペア）を生成する。この鍵対には、移動機ＭＳから電子銀行サーバＥＢＳに送信すべきデータの電子署名とその検証のための鍵対と、電子銀行サーバＥＢＳから移動機ＭＳへ送信すべきデータの暗号・復号のための鍵対との２種類のものがある。この鍵対の有効期限は、電子口座番号の有効期限と同一である。そして、申請局サーバＲＡは、「電子口座番号」とともに、作成した鍵対のうちの電子署名を検証するための公開鍵及び暗号化を行うための公開鍵を、認証局サーバＣＡに送付し、これらの鍵に対する公開鍵証明書を発行することを依頼する（矢印④）。

【００５８】これに応じて、認証局サーバＣＡは、電子署名検証用及び暗号用の公開鍵証明書を発行し、これらを「電子口座番号」と関連付けてディレクトリサーバＤＳに登録する（矢印⑤）。

【００５９】一方、電子銀行サーバＥＢＳは、ディレクトリサーバＤＳにアクセスして「電子口座番号」をキーにして検索することにより、電子署名検証用及び暗号用の公開鍵証明書が登録されたことを確認する（矢印⑥）。これは、電子銀行サーバＥＢＳと移動機ＭＳとの間でセキュリティが確保された通信を行うことが可能になったことを意味する。

【００６０】そして、電子銀行サーバＥＢＳは、「電子口座番号」を指定して、その番号が示す電子口座を使用してもよい旨を申請局サーバＲＡに通知する（矢印⑦）。

【００６１】これに応じて、申請局サーバＲＡは、ディレクトリサーバＤＳにアクセスし、そこに予め格納されている「電子銀行署名検証用証明書」、「電子銀行向け暗号用証明書」、「認証局署名検証用証明書」を取得する（矢印⑧）。

【００６２】そして、申請局サーバＲＡは、ＵＩＭ１に対し、図示せぬＲＯＭライタを介して、「署名用秘密鍵」、「復号用秘密鍵」、「電子銀行署名検証用証明書」、「電子銀行向け暗号用証明書」、「認証局署名検証用証明書」、「電子銀行ＩＤ」及び「電子口座番号」を書き込む。ユーザは、これらの情報が書き込まれたＵＩＭ１を受け取り、これを移動機ＭＳに装着して処理は終了する（矢印⑨）。

【００６３】（２）電子口座の継続

上述のようにしてユーザは電子口座を開設することができるが、一度開設した電子口座は定期的に口座管理料を支払うことにより継続使用が可能となる。この口座管理料の支払いの形態は以下のようなものがある。即ち、

（Ａ）ユーザの電子口座から口座管理料相当の電子バリューを引き落とす、（Ｂ）ユーザの実際の銀行口座から口座管理料相当の金額を引き落とす、（Ｃ）ＵＩＭ１の再購入代金のうち、その一部を口座管理料相当に充当する、（Ｄ）ＵＩＭ１への新しい鍵のインストール費用のうち、その一部を口座管理料相当に充当する、（Ｅ）ＵＩＭ１内で再作成した鍵対の公開鍵証明書発行費用のうち、その一部を口座管理料相当に充当する、という５方式がある。

【００６４】前述のとおり、ＵＩＭ１内の鍵は定期的に新しく更新されるようになっている。これは、公開鍵暗号アルゴリズムに基づく鍵を利用するシステムにおいては、鍵の安全性を確保するために、鍵に有効期限を設定し定期的に更新することが一般的である、という理由によるものである。この具体的な更新の方式については、（ア）ＵＩＭ１の再購入、（イ）申請局サーバＲＡにおけるＵＩＭ１へのリライト（再書き込み）、（ウ）認証局サーバＣＡから移動機ＭＳ内のＵＩＭ１へのオンラインダウンロード、（エ）ＵＩＭ１内で新たに生成し、認証局サーバＣＡに対しオンラインで公開鍵証明書の発行を依頼する、という４方式がある。

【００６５】ここで、ＵＩＭ１の更新の一例として、口座管理料を電子口座から電子バリューを引き落として電子銀行サーバＥＢＳに支払う方式（上記（Ａ））において、認証局サーバＣＡが生成する新しい鍵対のうちの秘密鍵を移動機ＭＳがオンラインでダウンロードする方式（上記（ウ））について、以下、図１３に示すシーケンスを参照しながら説明する。

【００６６】電子銀行サーバＥＢＳは、電子口座の継続利用を希望するユーザに対し、事前に口座管理料の引き落とし期日と金額を通知しておく。そして、期日が到来すると、電子銀行サーバＥＢＳは、ユーザの電子口座から、次期分の口座管理料として電子バリューを引き落とす（ステップＳ１）。

【００６７】次いで、電子銀行サーバＥＢＳは、ユーザの「電子口座番号」に対し、電子署名を施したうえで暗号化して申請局サーバＣＡに通知し、鍵対再発行、ユーザに対する秘密鍵のダウンロード許可、公開鍵証明書発行を依頼する（ステップＳ２）。

【００６８】一方、認証局サーバＣＡは、復号化と電子署名検証により、上記依頼が正しい電子銀行サーバＥＢＳからのものであることを確認したのち、鍵対を生成し、生成した公開鍵の証明書を発行する。発行した公開鍵証明書は、ディレクトリサーバＤＳに登録される（ス

テップＳ３）。

【００６９】電子銀行サーバＥＢＳは、ディレクトリサーバＤＳにアクセスして、新しい公開鍵証明書が発行できたことを確認すると（ステップＳ４）、継続利用するユーザの移動機ＭＳに対して、口座管理料を受領したことと秘密鍵をダウンロードする準備が整ったことを通知する（ステップＳ５）。

【００７０】移動機ＭＳは、電子銀行サーバＥＢＳから秘密鍵をダウンロードする準備が整った通知を受信すると、この通知を表示したのち、ユーザの操作に応じて認証局サーバＣＡに対し新しい秘密鍵のダウンロードを依頼する（ステップＳ６）。

【００７１】認証局サーバＣＡは、移動機ＭＳからダウンロードの依頼を受け取ると、新しい秘密鍵をユーザの古い（現在有効な）暗号用公開鍵で暗号化し、電子署名を施して移動機ＭＳに送信する（ステップＳ７）。

【００７２】移動機ＭＳは、認証局サーバＣＡから受信した新しい秘密鍵に施された電子署名を検証し、確かに正しい認証局サーバＣＡから送られてきたことを確認する。また、現在有効な「復号用秘密鍵」で、送られてきた秘密鍵を復号化する（ステップＳ８）。

【００７３】次いで、移動機ＭＳは、ＵＩＭ１内の古い秘密鍵を新しい秘密鍵に置き替える（ステップＳ９）。そして、移動機ＭＳは、認証局サーバＣＡに対し、秘密鍵の置き換えに成功した旨のメッセージを新しい「署名用秘密鍵」で署名して送信する（ステップＳ１０）。

【００７４】一方、認証局サーバＣＡは、秘密鍵の置き換えに成功した旨のメッセージを受信すると、古い秘密鍵に対する公開鍵をディレクトリサーバＤＳのＣＲＬに登録する（ステップＳ１１）。これにより、古い秘密鍵に対する公開鍵は使用不可能になる。

【００７５】（３）電子バリューの預け入れ・支払い

次に、図１４及び図１５に示すシーケンスを参照しながら、ＵＩＭ１もしくはプリペイドカードＰＣに対する電子バリューの預け入れ・支払いの動作について説明する。以下では、「電子口座の電子バリュー額」１０００円のうち、１００円を引き出してＵＩＭ１に充当する場合を例に挙げて説明する。まず、ユーザは、移動機ＭＳのキーパッドを操作して、プリペイドカードＰＣ内の電子バリューを利用するのか、移動機ＭＳに内蔵されたＵＩＭ１内の電子バリューを利用するのかを選択し、さらに電子口座から引き出したい金額あるいは電子口座に対して預け入れたい金額（即ち、取引金額）を入力する。ここでは、ＵＩＭ１が電子財布として選択され、引き出し金額１００円が入力される。移動機ＭＳは、上記キー操作を受け付ける（ステップＳａ１）。

【００７６】次いで、移動機ＭＳは、ステップＳａ１において入力された情報及びＵＩＭ１内の電子バリュー情報に対し、ＵＩＭ１に格納されている「電子銀行向け暗号用証明書」を用いて暗号化した後に「署名用秘密鍵」で電子署名を施し、さらにタイムスタンプを付与したうえで、これを要求信号として電子銀行サーバＥＢＳに送信する（ステップＳａ２）。

【００７７】電子銀行サーバＥＢＳは、上記要求信号を受信すると、受信した電子バリュー情報内の「電子口座番号」をキーにして、ディレクトリサーバＤＳから電子署名検証用の公開鍵証明書を取得し、これを用いて移動機ＭＳの電子署名の正当性を検証する（ステップＳａ３）。

【００７８】次いで、電子銀行サーバＥＢＳは、自身が記憶している「復号用秘密鍵」を用いて、ステップＳａ２で受信した暗号文を復号し、さらにタイムスタンプを確認する（ステップＳａ４）。このタイムスタンプの確認とは、同一ユーザから同一のタイムスタンプが付与された要求信号が２つ以上存在しないことを確認する処理である。この処理により、要求信号の不正再送の危険性を防止することができる。

【００７９】次いで、電子銀行サーバＥＢＳは、指定された引き出し金額あるいは預け入れ金額を確認し、引き出しあるいは預け入れ後における、「ＵＩＭの電子バリュー額」、「電子口座の電子バリュー額」を計算する（ステップＳａ５）。ここでは、引き出し後の「ＵＩＭの電子バリュー額」は１００円となり、「電子口座の電子バリュー額」は９００円となる

【００８０】次に、電子銀行サーバＥＢＳは、「電子口座番号」をキーにしてディレクトリサーバＤＳから暗号用の公開鍵証明書を取得する（ステップＳａ６）。

【００８１】そして、電子銀行サーバＥＢＳは、ステップＳａ５における計算値のほか、「電子口座番号」、ユーザ名、引き出しまたは預け入れの別を示す取引種別及び取引金額に対し、ディレクトリサーバＤＳから取得した暗号用の公開鍵証明書を用いて暗号化を行う（ステップＳａ７）。

【００８２】さらに、電子銀行サーバＥＢＳは、上記暗号文に対し、自身が記憶している「署名用秘密鍵」を用いて電子署名を施したうえでタイムスタンプを付与して移動機ＭＳに送信する（ステップＳａ８）。

【００８３】移動機ＭＳは、受信したデータに対し、電子署名の検証、暗号文の復号、タイムスタンプの確認を実行する（ステップＳａ９）。

【００８４】移動機ＭＳは、引き出しあるいは預け入れ後の「ＵＩＭの電子バリュー額」及び「電子口座の電子バリュー額」を表示する（ステップＳａ１０）。ここでは、「ＵＩＭの電子バリュー額」は１００円となり、「電子口座の電子バリュー額」は９００円となる。ユーザは、これを目視確認し、自身の要求と整合するものであるか否かを示すＯＫ又はＮＧのキー操作を行う。

【００８５】ここでＯＫのキー操作がなされた場合、移動機ＭＳは、ＵＩＭ１に記憶されている電子バリュー情報を更新する（ステップＳａ１１）。即ち、図８に示す

「電子口座の電子バリュー額」を１０００円から９００円に更新し、「ＵＩＭの電子バリュー額」を０円から１００円に更新し、「カレント電子バリュー額」を０円から１００円に更新したうえで、受信したタイムスタンプと電子署名とをそれぞれ、「電子バリュー額更新時タイムスタンプ」と「電子銀行署名ＳＧＮ２」として格納する。

【００８６】そして、移動機ＭＳは、ＯＫのキー操作がなされたということを示すメッセージを作成し、このメッセージに対して、ステップＳａ２と同様に「電子銀行向け暗号用証明書」による暗号化、「署名用秘密鍵」による電子署名、タイムスタンプ付与の処理を行ったうえで電子銀行サーバＥＢＳに送信する（ステップＳａ１２）。

【００８７】次に、図１５において、電子銀行サーバＥＢＳは、上記メッセージを受信すると、ステップＳａ３と同様に、ディレクトリサーバＤＳから「電子署名検証用証明書」を取得し、これを用いて電子署名の正当性を検証する（ステップＳａ１３）。 さらに、電子銀行サーバＥＢＳは、ステップＳａ４と同様に、「復号用秘密鍵」を用いて暗号文を復号し、タイムスタンプを確認する（ステップＳａ１４）。

【００８８】この結果、電子銀行サーバＥＢＳは、ＯＫの旨を示すメッセージを確認した場合には、図４に示す電子バリュー管理情報を更新する（ステップＳａ１５）。ここでは、「電子口座の電子バリュー額」を１０００円から９００円に更新し、「ＵＩＭの電子バリュー額」を０円から１００円に更新し、電子口座のカレント電子バリュー額を１０００円から９００円に更新し、ＵＩＭのカレント電子バリュー額を０円から１００円に更新したうえで、この時点のタイムスタンプを発行し、これを「電子バリュー額更新時タイムスタンプ」及び「カレント電子バリュー額更新時タイムスタンプ」として格納する。

【００８９】そして、電子銀行サーバＥＢＳは、取引が完了した旨のメッセージを移動機ＭＳに送信する（ステップＳａ１６）。一方、移動機ＭＳは、受信したメッセージを表示し（ステップＳａ１７）、処理は終了する。

【００９０】上記の例において、ステップＳａ１０におけるキー操作がＮＧの場合は、移動機ＭＳは、ＵＩＭ１内の電子バリュー情報を更新しない。そして、ステップＳａ１２において、ＮＧの旨を示すメッセージを作成し、電子銀行サーバＥＢＳに送信する。そして、電子銀行サーバＥＢＳは、ＮＧのメッセージを受信すると、ステップＳａ１３において、電子バリュー管理情報を更新せずに処理を終了する。ただし、電子銀行サーバＥＢＳは、上記の処理にかかるログを移動機ＭＳの電子署名とともに保管しておく。これは、後で移動機ＭＳのユーザから「確認結果としてＯＫを入力したはずだ」というようなクレーム等に対処するために使用する。

【００９１】さて、例えばステップＳａ１２における移動機ＭＳからのメッセージを電子銀行サーバＥＢＳが受信できない等の理由によって上記処理が完了しない場合は、電子銀行サーバＥＢＳは、移動機ＭＳに対し、取引が完了しなかった旨の不完了メッセージ、及び取引前のＵＩＭ１内の電子バリュー額に対し、ステップＳａ８と同様に、暗号化した上で電子署名を施し、タイムスタンプを付与して移動機ＭＳに送信する。一方、移動機ＭＳは、不完了メッセージを電子銀行サーバＥＢＳから受信した場合、そのメッセージを表示し、「ＵＩＭの電子バリュー額」を、不完了メッセージと共に送られてきた取引前の「ＵＩＭの電子バリュー額」に置き換える。

【００９２】また、例えば長期間に渡る通信遮断等により、移動機ＭＳが完了メッセージ又は不完了メッセージのどちらも受信できなかった場合は、移動機ＭＳは、取引未完了の旨を示すメッセージを表示部に表示する。ユーザは、通信遮断等から復旧後、移動機ＭＳを操作して電子銀行サーバＥＢＳに通信接続し、更新後の電子バリュー情報を取得して自身の電子バリュー情報を更新する。

【００９３】上記の例においては、移動機ＭＳのＵＩＭ１内の電子バリューを例にあげて説明したが、プリペイドカードＰＣ内の電子バリューを電子口座に預入れするような場合、プリペイドカードＰＣは赤外線通信を行うことにより移動機ＭＳを介して上記と同様の処理を行えばよい。

【００９４】（４）電子財布間のやり取り

移動機ＭＳは、赤外線通信のような、電子銀行サーバＥＢＳを介在しないローカルな通信手段により、電子バリューをやり取りすることができる。以下では、図１６及び図１７に示すシーケンスを参照しながら、ユーザＡの移動機ＭＳ１から１００円の電子バリューを支払って、ユーザＢの移動機ＭＳ２がこれを受け取る場合を例に挙げて動作説明を行う。

【００９５】まず、ユーザＡのキー操作に応じて、移動機ＭＳ１は、ユーザＢの移動機ＭＳ２に対し、ユーザＢの電子バリュー情報の中の「電子銀行ＩＤ」、「電子財布種別」、「電子口座番号」及びこれらに対する「電子銀行署名ＳＧＮ１」を要求する要求信号を赤外線により送信する（ステップＳｂ１）。

【００９６】ユーザＢの移動機ＭＳ２は、この要求信号を受信すると、自身のＵＩＭ１から要求された電子バリュー情報を読み出し、これを移動機ＭＳ１に赤外線通信により送信する（ステップＳｂ２）。

【００９７】移動機ＭＳ１は、受信した電子バリュー情報の中の「電子銀行署名ＳＧＮ１」を検証し、ユーザＢが電子銀行サーバＥＢＳが発行する電子バリューの正当な持ち主であることを確認する（ステップＳｂ３）。確認できない場合は、処理を終了する。

【００９８】次に、ユーザＡは、ユーザＢに対して支払

う電子バリュー金額１００円と、電子バリューを支払う「電子財布種別」（ここでは、ＵＩＭ１とする）を入力した後、支払いを指示するキー操作を行う。移動機ＭＳ１は、このキー操作を受け付ける（ステップＳｂ４）。

【００９９】次いで、移動機ＭＳ１は、ユーザＢの「電子口座番号」、ユーザＡの「電子口座番号」及び「取引金額」（ここでは、移動機ＭＳ１から移動機ＭＳ２へ支払われる電子バリュー額１００円）を情報セットにし、この情報セットに対してユーザＡの電子署名を施して、「ユーザＡが支払う電子バリュー情報」として移動機ＭＳ２に送信する。この際、移動機ＭＳ１は、自身が記憶している電子バリュー情報の中のユーザＡの「電子銀行ＩＤ」、「電子財布種別」、「電子口座番号」及びこれらに対する「電子銀行署名ＳＧＮ１」も合わせて送信する（ステップＳｂ５）。

【０１００】移動機ＭＳ２は、受信した「電子銀行署名ＳＧＮ１」を検証し、ユーザＡが電子銀行サーバＥＢＳの発行する電子バリューの正当な持ち主であることを確認する（ステップＳｂ６）。確認できない場合は、処理を終了する。

【０１０１】さらに、移動機ＭＳ２は、受信した情報セットに対して施されたユーザＡの電子署名を検証する（ステップＳｂ７）。これにより、第３者がユーザＡの移動機ＭＳ１へなりすますことを防止することが可能となる。

【０１０２】次いで、移動機ＭＳ２は、受信した「Ａが支払う電子バリュー情報」のうちユーザＡの電子署名を除く情報を表示する（ステップＳｂ８）。即ち、ここでは、ユーザＢの「電子口座番号」、ユーザＡの「電子口座番号」及び「取引金額」１００円が表示されることになる。ユーザＢは、この表示を参照し、問題がなければ、ＯＫである旨の指示を移動機ＭＳ２に入力する。一方、問題がある場合は、ユーザＢは、ＮＧである旨の指示を移動機ＭＳ２に入力する。移動機ＭＳ２は、ＮＧである旨を移動機ＭＳ１に通知し、処理を終了する。

【０１０３】次に、移動機ＭＳ２は、自身のＵＩＭ１内に記憶されている電子バリュー情報の中の「ＵＩＭのカレント電子バリュー額」に対し、「取引金額」に相当する電子バリュー額１００円を追加し、移動機ＭＳ１から受け取った「Ａが支払う電子バリュー情報」に基づいて「電子バリュー更新履歴」に更新履歴を追加する（ステップＳｂ９）。

【０１０４】次に、移動機ＭＳ２は、「Ａが支払う電子バリュー情報」のうちユーザＡの電子署名を除く情報、即ち、ユーザＢの「電子口座番号」、ユーザＡの「電子口座番号」及び「取引金額」１００円に対してユーザＢの電子署名を施し、これを「Ｂが受け取った電子バリュー情報」として移動機ＭＳ１に送信する（ステップＳｂ１０）。

【０１０５】移動機ＭＳ１は、「ユーザＢが受け取った電子バリュー情報」を受信すると、これに施されているユーザＢの電子署名を検証する（ステップＳｂ１１）。

【０１０６】次に、移動機ＭＳ１は、自身のＵＩＭ１に記憶している電子バリュー情報の中の「ＵＩＭのカレント電子バリュー額」から「取引金額」に相当する電子バリュー額１００円を減額し、「ユーザＢが受け取った電子バリュー情報」に基づいて「電子バリュー更新履歴」に更新履歴を追加する（ステップＳｂ１２）。この時点で、移動機ＭＳ１と移動機ＭＳ２との間のローカルな電子バリューのやり取りは完了することになる。

【０１０７】次に、図１７に示すシーケンスは、電子バリューの支払いを受けたユーザＢの移動機ＭＳ２が、図１６に示す処理を終了した後、電子銀行サーバＥＢＳと通信する必要が生じた際に開始される。まず、移動機ＭＳ２は、自身のＵＩＭ１から、「電子バリュー更新履歴」を読みだし、これを電子銀行サーバＥＢＳに送信して取引の正当性を確認することを依頼する（ステップＳｃ１）。

【０１０８】一方、電子銀行サーバＥＢＳサーバは、移動機ＭＳ２から受信した「電子バリュー更新履歴」を参照し、この「電子バリュー更新履歴」内の「取引相手電子署名」、ここではユーザＡの電子署名を検証する。この検証の結果、問題がなければ、以下の電子バリュー管理情報を変更する（ステップＳｃ２）。即ち、電子バリュー受取側であるユーザＢに対応した電子バリュー管理情報に関しては、「ＵＩＭの電子バリュー額」に１００円を追加し、「電子バリュー額更新時タイムスタンプ」を更新し、「ＵＩＭのカレント電子バリュー額」に１００円を追加し、「カレント電子バリュー額更新時タイムスタンプ」を更新する処理を行う。また、電子バリューの支払い側であるユーザＡに対応した電子バリュー管理情報に関しては、「ＵＩＭのカレント電子バリュー額」を１００円減額し、「カレント電子バリュー額更新時タイムスタンプ」を更新する処理を行う。なお、電子銀行サーバＥＢＳは、「取引相手電子署名」の検証結果に問題がある場合は、問題があるため更新できなかった旨のメッセージを作成し、電子銀行サーバＥＢＳの管理者に通知する。

【０１０９】さて、電子銀行サーバＥＢＳは、ステップＳｃ２において更新した電子バリュー管理情報に基づいて、更新すべき電子バリュー情報を移動機ＭＳ２に送信する（ステップＳｃ３）。ここで送信される電子バリュー情報は、「ＵＩＭの電子バリュー額」、「電子バリュー額更新時タイムスタンプ」、「電子銀行署名ＳＧＮ２」である。ここで、上記のように「取引相手電子署名」の検証結果に問題がある場合は、上述したような、問題があるため更新できなかった旨のメッセージも合わせて移動機ＭＳ２に送信する。

【０１１０】移動機ＭＳ２は、電子銀行サーバＥＢＳから受信した電子バリュー情報に応じて、ＵＩＭ１内の電

子バリュー情報を更新する（ステップＳｃ４）。

【０１１１】さて、移動機ＭＳ１は、移動機ＭＳ２と同様に、後に発生した処理において電子銀行サーバＥＢＳと通信する際に、電子銀行サーバＥＢＳから自身の電子バリュー情報のチェックを受ける。即ち、電子銀行サーバＥＢＳは、移動機ＭＳ１からのアクセスを受けた際に、ユーザＡに対応した「電子バリュー管理情報」のうち、「ＵＩＭのカレント電子バリュー額」と「ＵＩＭの電子バリュー額」を比較する。もし、両者が異なるようであれば電子バリュー管理情報を更新する。ここでの更新内容は、「ＵＩＭの電子バリュー額」を「ＵＩＭのカレント電子バリュー額」に合わせることと、「電子バリュー額更新時タイムスタンプ」を更新することである。

【０１１２】上述した電子バリュー管理情報の更新内容に合わせて、電子銀行サーバＥＢＳは、移動機ＭＳ１に対し、更新すべき電子バリュー情報を送信する。即ち、「ＵＩＭの電子バリュー額」、「電子バリュー額更新時タイムスタンプ」、「電子銀行署名ＳＧＮ２」を送信する。

【０１１３】移動機ＭＳ１は、電子銀行サーバＥＢＳから受信した電子バリュー情報のうち、「電子銀行署名ＳＧＮ２」を検証し、問題がなければ、ＵＩＭ１内の電子バリュー情報を更新する（ステップＳｂ２０）。以上の処理により、電子銀行サーバＥＢＳにより支払処理が保証され、完結することになる。

【０１１４】このように電子財布間のやり取りは、取引主体の電子財布の双方から「電子バリュー更新履歴」が電子銀行サーバＥＢＳに到着してはじめて有効な処理として完結する。しかし、これに限らず、どちらか一方の電子財布の「電子バリュー更新履歴」が通知されることのみによって、処理完結と判断してもよい。この場合、前述したように電子バリューを受け取った側の更新履歴ではなく、電子バリューを支払った側の更新履歴を電子銀行サーバＥＢＳに通知することによっても処理は完結できる。

【０１１５】なお、上記の例においては、支払い側の電子財布として移動機ＭＳのＵＩＭ１を例にあげて説明したが、プリペイドカードＰＣ内の電子バリューを用いることももちろん可能である。この場合、プリペイドカードＰＣは赤外線通信を行うことにより移動機ＭＳを介して上記と同様の処理を行えばよい。

【０１１６】（５）電子バリューの振り込み

電子バリューは、自分の電子財布または電子口座から他人の電子口座に対する振り込みという形で、他人に譲渡することができる。以下、図１８に示すシーケンスを参照しながら、電子バリューの振り込みについて説明する。

【０１１７】まず、ユーザは、移動機ＭＳを操作して、振り込む電子バリューの引き出し元（以下、振り込み元）を選択する。具体的には、プリペイドカードＰＣ、移動機ＭＳ内のＵＩＭ１、及びユーザ自身の電子口座、の３つから選択されることになるが、ここでは、ＵＩＭ１が選択されたものとする。次いで、ユーザは、振り込み先の「電子口座番号」（以下、振り込み先電子口座番号）及び振り込む金額（以下、振り込み金額）を入力する。移動機ＭＳは、以上のような入力操作を受け付ける（ステップＳｄ１）。

【０１１８】次いで、移動機ＭＳは、入力された情報に対して、タイムスタンプを付与し、電子銀行サーバ向け暗号用公開鍵による暗号化を行い、「署名用秘密鍵」を用いて電子署名を施したデータを、振込みを要求する要求信号として電子銀行サーバＥＢＳに送信する（ステップＳｄ２）。なお、ステップＳｄ１において、ユーザがプリペイドカードＰＣを振り込み元として選択した場合は、移動機ＭＳはプリペイドカードＰＣと赤外線通信を行ってプリペイドカードＰＣ内の電子バリュー情報を取得し、これも同時に電子銀行サーバＥＢＳに送信する。

【０１１９】一方、電子銀行サーバＥＢＳでは、受信した要求信号に対し、電子署名の検証、暗号文復号、タイムスタンプ確認により、不正がないことを確認する（ステップＳｄ３）。

【０１２０】次に、電子銀行サーバＥＢＳは、指定された振り込み先電子口座が入金可能あるいは開設状態で実在すること、及び振り込み元の電子バリューの残高が指定された振込金額以上であることを確認する（ステップＳｄ４）。なお、プリペイドカードＰＣが振り込み元として選択されている場合、電子銀行サーバＥＢＳは、「電子銀行署名ＳＧＮ４」を検証することにより、振り込み元（プリペイドカードＰＣ）の電子バリュー額に対して不正な改ざんがないことを確認した上で振り込み可能か確認する。

【０１２１】次に、電子銀行サーバＥＢＳは、振り込み後の振り込み元（ここではＵＩＭ１）の電子バリュー額を計算する。そして、「電子銀行ＩＤ」、振り込み先電子口座番号、振り込み先電子口座のユーザ名、振り込み金額、振り込み元のユーザの「電子口座番号」、振り込み前後の振り込み元（ＵＩＭ１）の電子バリュー額に対し、タイムスタンプを付与し、ディレクトリサーバＤＳから取得した暗号用公開鍵による暗号化を行い、自身が記憶する「署名用秘密鍵」で電子署名を施して移動機ＭＳに送信する（ステップＳｄ５）。

【０１２２】移動機ＭＳは、受信したデータについて、電子署名検証、暗号文復号、タイムスタンプ確認により、不正がないことを確認する（ステップＳｄ６）。

【０１２３】次いで、移動機ＭＳは、受信したデータを表示する。ユーザがこれを目視確認し、ＯＫあるいはＮＧを示す入力操作を行うと、移動機ＭＳはこれを受け付ける（ステップＳｄ７）。ここで、ＯＫを示す入力操作がなされた場合、振り込み元として選択したＵＩＭ１が記憶している電子バリュー情報を更新する。ここで、更

新される電子バリュー情報は、「ＵＩＭの電子バリュー額」、「電子バリュー額更新時タイムスタンプ」、「電子銀行署名ＳＧＮ２」及び「カレント電子バリュー額」である。なお、振り込み元として電子口座を選択した場合は、電子財布内の情報は更新されない。また、ＮＧを示す入力操作がなされた場合は、電子財布内の電子バリューは更新されない。

【０１２４】次いで、移動機ＭＳは、受け付けた入力操作がＯＫであるかＮＧであるかを示すメッセージを作成し、このメッセージに対し、タイムスタンプ付与、電子銀行向け暗号用公開鍵による暗号化、「署名用秘密鍵」による電子署名を施し、電子銀行サーバＥＢＳに送信する（ステップＳｄ８）。

【０１２５】電子銀行サーバＥＢＳがＯＫの旨のメッセージを受信した場合は、振り込み先電子口座内の電子バリュー額を計算し、この計算値を電子銀行サーバＥＢＳの電子署名を施して、振込先の電子口座に対応した電子バリュー管理情報として格納する（ステップＳｄ９）。なお、振り込み元として電子口座を選択した場合は、振り込み元電子口座内の電子バリュー額を計算し、この計算値に電子銀行サーバＥＢＳの電子署名を施して電子バリュー管理情報として格納する。

【０１２６】電子銀行サーバＥＢＳは、処理が終了した旨のメッセージを移動機ＭＳに送信する（ステップＳｄ１０）。移動機ＭＳは、受信したメッセージを表示して、一連のやり取りの完了をユーザに通知する。

【０１２７】また、電子銀行サーバＥＢＳがＮＧの旨のメッセージを受信した場合は、電子バリュー管理情報を更新せずに処理を終了する。ただし、電子銀行サーバＥＢＳは、上記の処理にかかるログを移動機ＭＳの電子署名とともに保管しておく。これは、後で移動機ＭＳのユーザから「確認結果としてＯＫを入力したはずだ」というようなクレーム等に対処するために使用する。

【０１２８】さて、例えばステップＳｄ８における移動機ＭＳからのメッセージを電子銀行サーバＥＢＳが受信できない等の理由により上記処理が完了しない場合は、電子銀行サーバＥＢＳは、移動機ＭＳに対し、取引が完了しなかった旨の不完了メッセージ、及び取引前の「ＵＩＭの電子バリュー額」に対し、ステップＳａ８と同様に、暗号化した上で電子署名を施し、タイムスタンプを付与して移動機ＭＳに送信する。一方、移動機ＭＳは、不完了メッセージを電子銀行サーバＥＢＳから受信した場合、そのメッセージを表示し、「ＵＩＭの電子バリュー額」を、不完了メッセージと共に送られてきた取引前の「ＵＩＭの電子バリュー額」に置き換える。

【０１２９】また、例えば長期間に渡る通信遮断等により、移動機ＭＳが完了メッセージ又は不完了メッセージのどちらも受信できなかった場合は、移動機ＭＳは、取引未完了の旨を示すメッセージを表示部に表示する。ユーザは、通信遮断等から復旧後、移動機ＭＳを操作して電子銀行サーバＥＢＳに通信接続し、更新後の電子バリュー情報を取得して自身の電子バリュー情報を更新する。

【０１３０】上記の例においては、移動機ＭＳのＵＩＭ１内の電子バリューを例にあげて説明したが、プリペイドカードＰＣ内の電子バリューを預入れするような場合には、プリペイドカードＰＣは赤外線通信を行うことにより移動機ＭＳを介して上記と同様の処理を行えばよい。

【０１３１】Ｃ：応用例

次に、実施形態の応用例について説明する。例えば自動販売機やＰＯＳ（Point Of Sale）レジに対し、移動機ＭＳのＵＩＭ１に相当する電子財布の機能を組み込み、顧客（即ち自動販売機等の利用者）の移動機ＭＳ（若しくはプリペイドカードＰＣ）と自動販売機との間で、ローカルな通信により電子財布間の電子バリュー受け渡しを行ない、キャッシュレスで商品を販売することができる。自動販売機においては、移動機ＭＳと電子バリューをやり取りする時点で「電子銀行署名ＳＧＮ１」を検証することにより、その正当性を確認することができるため、その都度電子銀行サーバＥＢＳに正当性を確認する必要がないといえる。したがって、顧客にとっては速やかに商品の購入ができるというメリットがあり、自動販売機等の業者にとってはサーバとの通信費が押さえられるというメリットがある。

【０１３２】また、自動販売機に移動機ＭＳの電子財布の機能を組み込まずに、顧客の移動機ＭＳと自動販売機等との間で、キャッシュレスで商品を販売することも可能である。この場合も、移動機ＭＳと電子バリューをやり取りする時点で「電子銀行署名ＳＧＮ１」を検証する。この例について、図１９を参照しながら説明する。自動販売機ＶＭは、移動通信網に接続された自販機サーバＶＳに有線或いは無線接続されている。自動販売機ＶＭには、移動機ＭＳと赤外線通信を行って通信を行う機能と、移動機ＭＳに送信するデータに電子署名を施す機能と、移動機ＭＳから送信される「電子銀行署名ＳＧＮ１」を検証する機能が搭載されている。

【０１３３】顧客の移動機ＭＳ１は、自動販売機ＶＭとの間の赤外線通信を用いて、自動販売機業者の「電子口座番号」を受け取る。

【０１３４】顧客は、自動販売機ＶＭに対して支払う電子バリュー金額と「電子財布種別」を、移動機ＭＳに入力し、次いで、支払い指示を示す操作をする。移動機ＭＳはこの入力操作を受け付ける。

【０１３５】移動機ＭＳは、自動販売機業者の「電子口座番号」、顧客の「電子口座番号」、及び支払う電子バリューに相当する金額情報をセットにし、これに対して顧客の電子署名を施して「顧客が支払う電子バリュー情報」として赤外線通信により自動販売機ＶＭに送信する。また、顧客の電子財布内に格納された電子バリュー

情報のうち、「電子銀行サーバＩＤ」、「電子財布種別」、「電子口座番号」及びこれらに対する「電子銀行署名ＳＧＮ１」の情報セットも同時に自動販売機ＶＭに送信する。

【０１３６】自動販売機ＶＭは、受信した「電子銀行署名ＳＧＮ１」を検証し、顧客が正しい電子銀行サーバＥＢＳが発行した電子バリューの持ち主であることを確認する。ここで、電子署名の検証結果がＮＧの場合は、顧客との処理を中止し、受け取った情報を不正なアクセスの可能性があるものとしてロギングする。

【０１３７】上記の電子署名検証がＯＫの場合、自動販売機ＶＭは、支払う電子バリューに相当する金額情報が商品金額以上であることを確認する。これが不足している場合は、自動販売機ＶＭは、移動機ＭＳとの処理を中止し、金額不足の旨のメッセージを移動機ＭＳに返信する。

【０１３８】上記の金額確認がＯＫの場合、自動販売機ＶＭは、受信した、自動販売機業者の「電子口座番号」、顧客の「電子口座番号」、支払う電子バリューに相当する金額情報及び顧客の電子署名を「電子バリュー更新履歴」としてロギングする。そして、自動販売機ＶＭは、商品代金を受領した旨のメッセージに電子署名を施して移動機ＭＳに返信する。この時点で自動販売機ＶＭに対する商品代金の支払いは完了し、自動販売機ＶＭでは商品選択のボタンを押下できる状態になり、商品の受け渡しが完了する。

【０１３９】そして、移動機ＭＳは、自動販売機ＶＭから受信したメッセージに基づいて、ＵＩＭ１内の電子バリュー情報を更新する。更新する情報は、「カレント電子バリュー額」から支払った商品代金を減額すること と、「電子バリュー更新履歴」に自動販売機業者の「電子口座番号」、顧客の「電子口座番号」、支払う電子バリューに相当する金額情報及び自動販売機ＶＭの電子署名を追加することである。

【０１４０】自動販売機ＶＭのロギング情報は、定期的に自販機サーバＶＳによって収集され、電子銀行サーバＥＢＳに送られる。

【０１４１】電子銀行サーバＥＢＳサーバでは、自販機サーバＶＳから受け取った「電子バリュー更新履歴」に対して、支払い者の電子署名を検証し、以下の管理情報を変更する。即ち、自動販売機ＶＭ業者の電子口座の電子バリュー管理情報については、「電子口座の電子バリュー額」追加、電子口座の「電子バリュー額更新時タイムスタンプ」更新の処理を行い、顧客の電子口座・電子財布の電子バリュー管理情報については、ＵＩＭ１の「カレント電子バリュー額」減額、「電子バリュー額更新時タイムスタンプ」更新の処理を行う。ここで、顧客がプリペイドカードＰＣで支払った場合においては、プリペイドカードＰＣについて、「プリペイドカードのカレント電子バリュー額」減額、「電子バリュー額更新時タイムスタンプ」更新の処理を行う。

【０１４２】なお、電子銀行サーバＥＢＳは、電子認証結果に問題がある場合は、問題があるため更新できなかった旨のメッセージを作成し、電子銀行サーバＥＢＳの管理者に通知する。

【０１４３】電子銀行サーバＥＢＳは、自動販売機ＶＭ業者の電子口座の電子バリュー管理情報について行った更新内容、即ち、「電子口座の電子バリュー額」追加、電子口座の「電子バリュー額更新時タイムスタンプ」更新内容を自販機サーバＶＳに送信する。また、電子認証結果に問題がある場合は、上述したメッセージも合わせて自販機サーバＶＳに送信する。

【０１４４】自販機サーバＶＳは、電子銀行サーバＥＢＳから受け取ったメッセージを表示するなどにより、これを自販機サーバＶＳの管理者に通知する。管理者は、問題があるため更新できなかった旨のメッセージを受け取った場合は、内容を確認した上で、詐欺行為と認められる場合は法的手段に訴えるなどの対処をする。

【０１４５】顧客の電子財布内の電子バリュー情報は、後に電子銀行サーバＥＢＳにアクセスした際に、前述した電子財布間のやり取りの手順と同様の手順により、支払い処理が電子銀行サーバＥＢＳに保証されて完結する。

【０１４６】なお、自動販売機ＶＭあるいは自販機サーバのシステムトラブルにより、顧客から受け取った「電子バリュー更新履歴」が失われた場合は、電子財布間のやり取りにおいて「電子バリュー更新履歴」が失われた場合と同様の方式により、カレント電子バリューとの整合性を保証する。

【０１４７】このように実施形態によれば、電子銀行サーバＥＢＳが、電子口座と電子財布との双方の電子バリュー額を管理するので、電子財布側で電子バリューが不正に書き換えられることを検出することができる。また、電子財布間でローカルに電子バリューをやり取りした場合、「電子銀行署名ＳＧＮ１」を検証することにより、その都度電子銀行サーバＥＢＳに問い合わせることなく、電子財布間のみでその正当性を確認できる。したがって、ネットワーク上のトラヒックを増加させる虞がない。また、電子銀行サーバＥＢＳは、少なくともいずれか一方の電子財布からの通知により、自身が管理している電子バリュー管理情報を更新するので、効率性が向上する。また、取引時にはタイムスタンプを付与するので、これを用いて不正再送を防止することができる。

【０１４８】Ｄ：変形例

既述の通り、本発明は上述した実施形態に限定されず、以下のような種々の変更が可能である。

（１）移動機ＭＳの形態

移動機ＭＳは、無線通信機能を内蔵する携帯端末であればよく、上述した携帯電話機のほかにも、携帯電話機に接続してデータ通信を行なうパーソナルコンピュータま

たはＰＤＡ（Personal Digital Assistants）等であってもよい。

【０１４９】（２）移動機、プリペイドカード、自動販売機の通信形態

実施形態では、移動機ＭＳ、プリペイドカードＰＣ、自動販売機ＶＳは互いに赤外線を用いた無線通信を行うようになっていたが、これに限らず、有線通信であってもよい、例えば、移動局５０は、シリアル信号の入出力を行う１６芯コネクタを一般に備えているが、これと同様のものをプリペイドカードＰＣや自動販売機ＶＳ側にも備え、これらコネクタを相互にケーブル接続することによりデータ通信を行うようにしてもよい。

【０１５０】（３）各サーバの設置形態

実施形態においては、電子銀行サーバＥＢＳは移動通信網ＭＮ上に設置され、申請局サーバＲＡ、認証局サーバＣＡ及びディレクトリサーバＤＳは、インターネットＩＮＥＴ上の設置されていた。しかし、これに限らず、各サーバの設置場所はいずれのネットワーク上でもよい。

【０１５１】（４）鍵対の生成

実施形態では、申請局サーバＲＡがユーザの鍵対をの生成し、ＵＩＭ１に書き込むようにしていたが、これに限らない。例えば、ＵＩＭ１の製造工場で作成し、予め書き込んでいてもよいし、ＵＩＭ１に実装された鍵対生成機能により作成してもよい。また、認証局サーバＣＡのような機関に鍵対生成を依頼し、これをダウンロードするような形態であってもよい。

【０１５２】（５）ＵＩＭ１若しくはプリペイドカードＰＣの記憶容量

前述したＵＩＭ１やプリペイドカードＰＣ等の電子財布は、記憶容量不足により全ての「電子バリュー更新履歴」を格納しきれない場合や、あるいはシステムトラブルにより「電子バリュー更新履歴」の記憶装置に障害が発生した場合がある。このような場合、「電子バリュー更新履歴」が失われることが想定される。また、悪意のある利用者により、自らが支払った「電子バリュー更新履歴」のみを削除するという形で、一部が失われる場合もある。ところで、実施形態では、支払い側・受け取り側どちらか一方の「電子バリュー更新履歴」が電子銀行サーバＥＢＳに送られると、支払い側・受け取り側双方について正しい電子バリュー値に更新できるようになっている。しかしながら、支払い側・受け取り側の双方の「電子バリュー更新履歴」が失われた場合は、電子銀行サーバＥＢＳは、電子バリューのやり取りを把握することができない。この場合は、やり取りそのものが行なわれなかったとするために、後に各電子財布が電子銀行サーバＥＢＳにアクセスしたタイミングにおいて、各電子財布における「ＵＩＭのカレント電子バリュー額」を電子銀行サーバＥＢＳが管理する「電子財布の電子バリュー金額」に合わせて整合性を取る処理を行なう。即ち、電子財布側の電子バリュー情報を強制的に電子銀行側の電子バリュー情報に整合させるのである。このような前提のもとでは、移動機ＭＳは、電子財布の記憶容量に相当する量「電子バリュー更新履歴」を蓄積したことを検出すると、それ以後の電子バリューを利用した取引時において、取引日時の古い順から「電子バリュー更新履歴」を消去してもよい。また、移動機ＭＳは、電子財布の記憶容量に相当する量「電子バリュー更新履歴」を蓄積したことを検出すると、その「電子バリュー更新履歴」を強制的に電子銀行サーバＥＢＳに送信するようにしてもよい。これにより、電子財布側の電子バリュー情報と電子銀行側の電子バリュー情報とを整合させる。また、移動機ＭＳは、電子財布の記憶容量に相当する量「電子バリュー更新履歴」を蓄積したことを検出すると、それ以後、電子バリューを利用した取引を行わないようにしてもよい。そして、その旨を表示部に表示させてユーザに通知する等の処理を行う。

【０１５３】（６）移動機ＭＳ及びプリペイドカードＰＣ間の通信手段

移動機ＭＳ及びプリペイドカードＰＣ間のローカルな通信手段は、上述した赤外線通信に限定されるわけではなく、これとは異なる無線通信手段、例えばブルートゥース（登録商標）であってもよい。もちろん、移動機ＭＳ及び自動販売機ＶＭ間の通信手段についても、同様に、赤外線以外の無線通信手段を用いることが可能である。

【０１５４】

【発明の効果】上述したように本発明によれば、電子口座内の電子バリューの残高を記憶するとともに、電子財布としての通信端末に格納される電子バリューの残高を記憶し、取引の内容に応じて通信端末内の電子バリューの残高を更新するので、通信端末側における電子バリューの不正書き換えを検出することができる（請求項１及び２４）。

【０１５５】また、第１の通信端末及び第２の通信端末が電子バリューを互いに送受信する場合、第１の通信端末又は第２の通信端末のうち少なくともいずれか一方から提供される取引ログにより、通信端末に格納される電子バリューの残高を更新する。即ち、取引ログを送信する通信端末はいずれか一方でよいので、効率性が向上されることになる（請求項２）。

【０１５６】また、第１の通信端末及び第２の通信端末が電子バリューを互いに送受信する場合、第１の通信端末は、送信する電子バリューに対し、この電子バリューを発行した発行主体の識別情報及び当該発行主体の電子署名付加する一方、第２の通信端末は、受信した発行主体の識別情報及び電子署名を検証することにより、受信した電子バリューの正当性を確認する。これにより、通信端末間のみで電子バリューの正当性が確認されることとなり、効率よくセキュリティを確保することができる（請求項９及び２０）。

【図面の簡単な説明】

【図１】　本発明の実施形態に係るシステム全体の構成を示すブロック図である。
【図２】　同実施形態における電子銀行サーバの構成を示すブロック図である。
【図３】　同実施形態における電子銀行サーバ内のデータベースの記憶内容を説明する図である。
【図４】　同実施形態における電子銀行サーバ内のデータベースの記憶内容を説明する図である。
【図５】　同実施形態における電子銀行サーバ内のデータベースの記憶内容を説明する図である。
【図６】　同実施形態における移動機の構成を示すブロック図である。
【図７】　同実施形態におけるＵＩＭの記憶内容を説明する図である。
【図８】　同実施形態におけるＵＩＭの記憶内容を説明する図である。
【図９】　同実施形態におけるＵＩＭの記憶内容を説明する図である。
【図１０】　同実施形態におけるプリペイドカードの記憶内容を説明する図である。
【図１１】　同実施形態におけるプリペイドカードの記憶内容を説明する図である。
【図１２】　電子口座を開設する動作を説明する図である。
【図１３】　同実施形態におけるシステム全体の動作を示すシーケンス図である。
【図１４】　同実施形態におけるシステム全体の動作を示すシーケンス図である。
【図１５】　同実施形態におけるシステム全体の動作を示すシーケンス図である。
【図１６】　同実施形態におけるシステム全体の動作を示すシーケンス図である。
【図１７】　同実施形態におけるシステム全体の動作を示すシーケンス図である。
【図１８】　同実施形態におけるシステム全体の動作を示すシーケンス図である。
【図１９】　同実施形態の応用例におけるシステム全体の構成を示すブロック図である。
【符号の説明】
ＰＣ・・・プリペイドカード（通信端末）、
ＭＳ・・・移動機（通信端末）、
１・・・ＵＩＭ（ＩＣカード）、
２・・・無線通信部（取引ログ通知手段、更新手段、識別情報交換手段）、
３・・・制御部（メモリ、ログ蓄積手段、取引ログ通知手段、判断手段、セキュリティ手段、更新手段、不可手段、確認手段）、
４・・・ユーザインタフェース、
５・・・赤外線通信部（送信手段、受信手段、取得手段）、
ＭＮ・・・移動通信網（ダウンロード手段）、
ＥＢＳ・・・電子銀行サーバ、
１１・・・通信部（ダウンロード手段、ログ取得手段）、
１２・・・制御部（財布残金管理手段、財布残金更新手段、電子認証手段）、
１３・・・データベース（電子口座保持手段、財布残金管理手段、財布残金記憶手段）、
ＢＳ・・・銀行システム、
ＲＡ・・・申請局サーバ、
ＣＡ・・・認証局サーバ、
ＤＳ・・・ディレクトリサーバ、
ＩＮＥＴ・・・インターネット、
ＶＭ・・・自動販売機、
ＶＳ・・・自動販売機サーバ、

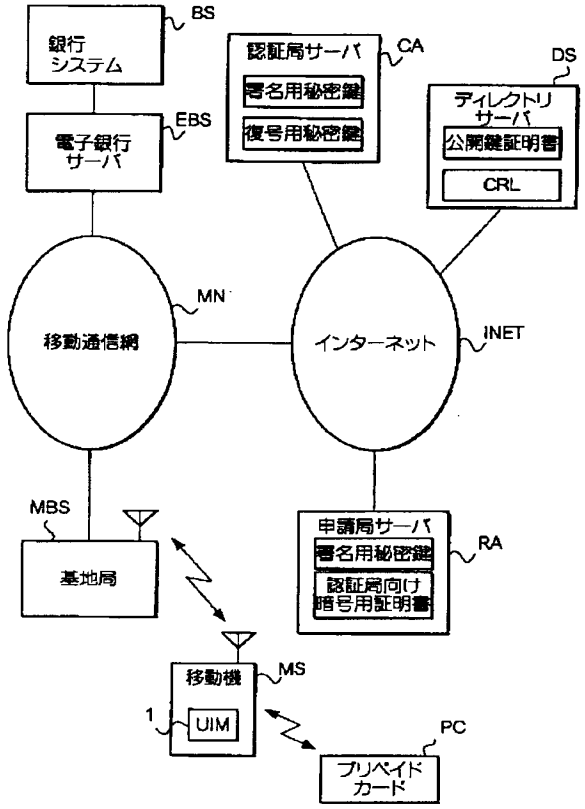
【図３】

通番	データ名	説明
1	署名用秘密鍵	電子銀行サーバEBSが送信するデータに対し電子署名を施すための秘密鍵
2	復号用秘密鍵	電子銀行サーバEBSが受信した暗号文を復号するための秘密鍵
3	認証局署名検証用証明書	認証局サーバ CA によって各種証明書に施された電子署名を検証するための公開鍵の証明書
4	電子バリュー管理情報	電子財布・電子口座の電子バリューを管理するための情報

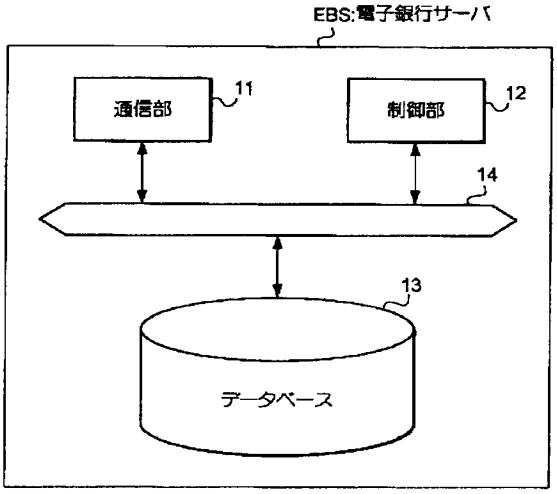
【図５】

通番	項目名	説明
1	電子銀行 ID	電子バリューを発行した電子銀行サーバ EBS の識別情報
2	プリペイドカード ID	プリペイドカードの識別情報
3	プリペイドカードの電子バリュー額	移動機 MS が最後に電子銀行サーバ EBS とアクセスした時点の電子口座の電子バリューの残高
4	電子バリュー額更新時タイムスタンプ	上記通番３の電子バリュー額を電子銀行サーバ EBS が更新した時点の電子銀行サーバ EBS が付与する日時情報
5	プリペイドカードのカレント電子バリュー額	現在のプリペイドカードの電子バリューの残高
6	カレント電子バリュー額更新時タイムスタンプ	上記通番５の電子バリュー額を電子銀行サーバ EBS が更新した時点の電子銀行サーバ EBS が付与する日時情報
7	電子バリュー更新履歴	プリペイドカードの所有者の移動機 MS が最後に電子銀行サーバ EBS とアクセスした時点から現在までのプリペイドカードの電子バリュー額の更新履歴

【図１】



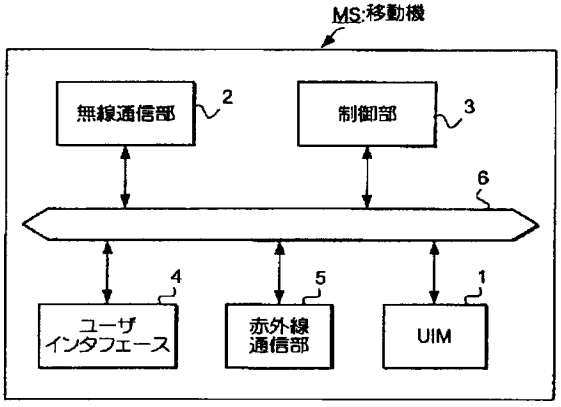
【図２】



【図４】

通番	データ名	説明
1	電子銀行 ID	電子バリューを発行した電子銀行サーバ EBS を識別するための識別情報
2	電子口座番号	電子口座の識別情報
3	電子口座の電子バリュー額	移動機 MS が最後に電子銀行サーバ EBS とアクセスした時点の電子口座の電子バリューの残高
4	UIM の電子バリュー額	移動機 MS が最後に電子銀行サーバ EBS とアクセスした時点における、UIM1 に格納されている電子バリューの残高
5	電子バリュー額更新時タイムスタンプ	上記通番 4 の電子バリュー額が電子銀行サーバ EBS によって更新された時点で付与される日時情報
6	電子口座のカレント電子バリュー額	電子口座内の最新の電子バリューの残高
7	UIM のカレント電子バリュー額	UIM1 に反映すべき電子バリューの残高
8	カレント電子バリュー額更新時タイムスタンプ	上記通番 6 及び 7 の電子バリュー額を電子銀行サーバ EBS が更新した時点で電子銀行サーバ EBS が付与する日時情報
9	電子バリュー更新履歴	移動機 MS が最後に電子銀行サーバ EBS とアクセスした時点から現在までの UIM の電子バリュー額の更新履歴

【図６】



【図７】

通番	データ名	説明
1	署名用秘密鍵	移動機 MS が送信するデータに対し、電子署名を施すための秘密鍵
2	復号用秘密鍵	移動機 MS が受信した暗号文を復号するための秘密鍵
3	電子銀行署名検証用証明書	電子銀行サーバ EBS によって施された電子署名を検証するための公開鍵の証明書
4	電子銀行向け暗号用証明書	電子銀行サーバ EBS へ送信するデータを暗号化するための公開鍵の証明書
5	認証局署名検証用証明書	認証局 CA によって各種証明書上に施された電子署名を検証するための公開鍵の証明書
6	ユーザ ID	移動機ユーザの識別情報
7	電子バリュー情報	UIM1 及び電子口座内の電子バリューに関する情報

【図８】

通番	データ名	説明
1	電子銀行 ID	電子バリューを発行した電子銀行を特定するための識別情報
2	電子財布種別	電子財布が UIM1 であるかプリペイドカード PC であるかという種別を示す情報
3	電子口座番号	電子銀行サーバ EBS において電子口座を特定するための識別情報
4	電子銀行署名 SGN1	上記通番 1～3 の残項目に改ざんがないことを保証するために、電子銀行サーバ EBS が付与する電子署名
5	電子口座の電子バリュー額	移動機 MS が最後に電子銀行サーバ EBS とアクセスした時点における電子口座の電子バリューの残高
6	UIM の電子バリュー額	移動機 MS が最後に電子銀行サーバ EBS とアクセスした時点における、UIM1 に格納されている電子バリューの残高
7	電子バリュー額更新時タイムスタンプ	UIM1 内の電子バリュー額が更新された時点で、電子銀行サーバ EBS によって付与された日時情報
8	電子銀行署名 SGN2	上記通番 1～3 及び 5～7 の全項目に改ざんがないことを保証するために、電子銀行サーバ EBS が付与する電子署名
9	カレント電子バリュー額	最新の UIM1 内の電子バリューの残高
10	電子バリュー更新履歴	移動機 MS が最後に電子銀行サーバ EBS とアクセスした時点から現在までの UIM1 の電子バリュー額の更新履歴

【図９】

通番	データ名	説明
1	受取側電子口座番号	電子バリューを受け取る側の電子口座番号
2	支払側電子口座番号	電子バリューを支払う側の電子口座番号
3	支払側プリペイドカード ID	電子バリューの支払がプリペイドカードの場合における、プリペイドカード ID
4	取引金額	電子バリューの受取側と支払側とで取引された金額
5	取引相手電子署名	取引相手の電子署名

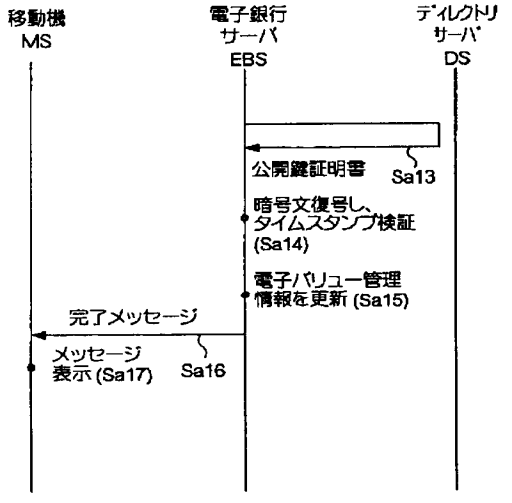
【図１０】

通番	データ名	説明
1	電子銀行署名検証用証明書	電子銀行サーバ EBS によって施された電子署名を検証するための公開鍵の証明書
2	電子銀行向け暗号用証明書	電子銀行サーバ EBS へ送信するデータを暗号化するための公開鍵の証明書
3	認証局署名検証用証明書	認証局 CA によって各種証明書上に施された電子署名を検証するための公開鍵の証明書
4	電子バリュー情報	プリペイドカード PC 内の電子バリューに関する情報

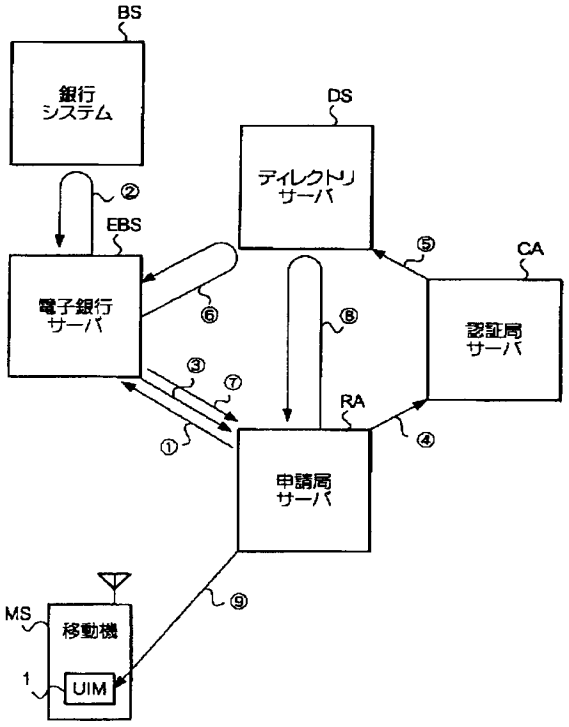
【図１１】

通番	データ名	説明
1	電子銀行 ID	電子バリューを発行した電子銀行サーバ EBS を識別するための識別情報
2	電子財布種別	電子財布が UIM1 であるかプリペイドカード PC であるかという種別を示す情報
3	プリペイドカード ID	プリペイドカード PC を特定するための識別情報
4	電子銀行署名 SGN3	上記通番 1～3 の全てが改ざんされていないことを保証するために電子銀行サーバ EBS が付与した電子署名
5	プリペイドカードの電子バリュー額	プリペイドカード PC の所有者の移動機 MS が最後に電子銀行サーバ EBS とアクセスした時点における、プリペイドカード PC に格納されている電子バリューの残高
6	電子バリュー額更新時タイムスタンプ	上記通番 4 の電子バリュー額が電子銀行サーバ EBS によって更新された時点で付与される日時情報
7	電子銀行署名 SGN4	上記通番 1～3 及び 5～7 の全てが改ざんされていないことを保証するために電子銀行サーバ EBS が付与した電子署名
8	カレント電子バリュー額	プリペイドカード PC 内の最新の電子バリュー額
9	電子バリュー更新履歴	移動機 MS が最後に電子銀行サーバ EBS とアクセスした時点から現在までのプリペイドカードの電子バリュー額の更新履歴

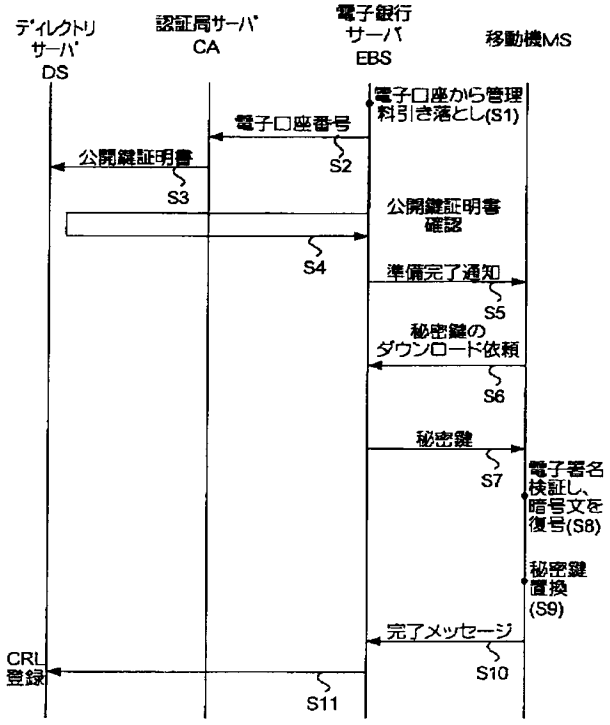
【図１５】



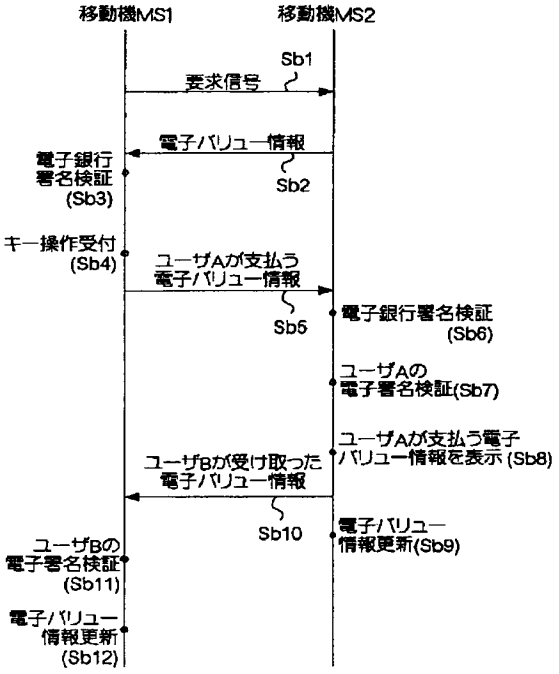
【図１２】



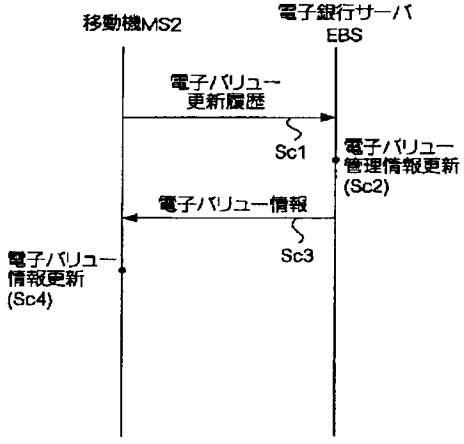
【図１３】



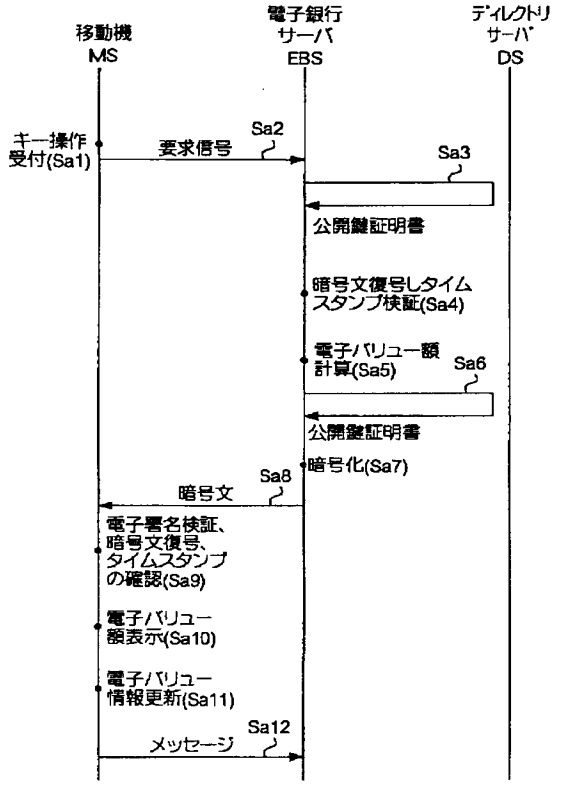
【図１６】



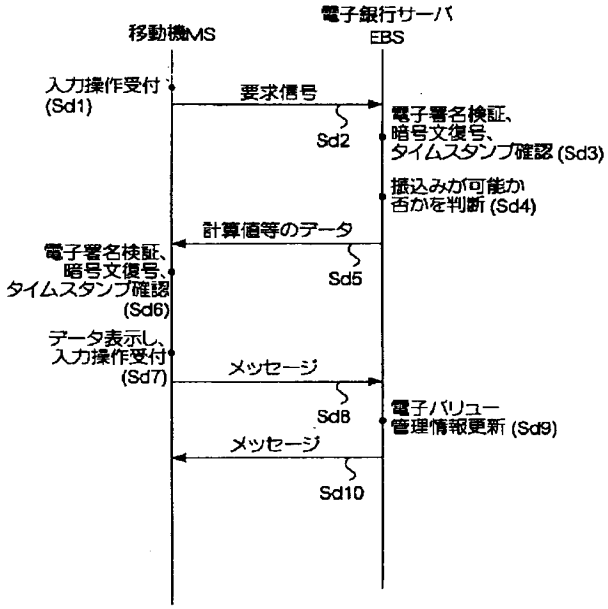
【図１７】



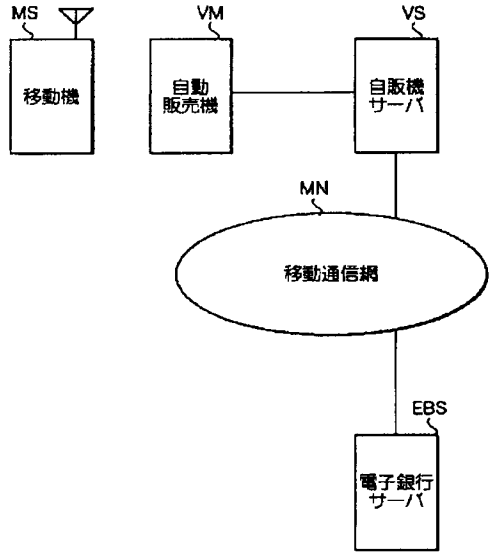
【図１４】


移動機
MS
電子銀行
サーバ
EBS
ディレクトリ
サーバ
DS
キー操作
受付(Sa1)
要求信号
Sa2
Sa3
公開鍵証明書
暗号文復号しタイム
スタンプ検証(Sa4)
電子バリュー額
計算(Sa5)
Sa6
公開鍵証明書
暗号化(Sa7)
Sa8
暗号文
電子署名検証、
暗号文復号、
タイムスタンプ
の確認(Sa9)
電子バリュー
額表示(Sa10)
電子バリュー
情報更新(Sa11)
Sa12
メッセージ

【図１８】


移動機MS
電子銀行サーバ
EBS
入力操作受付
(Sd1)
要求信号
Sd2
電子署名検証、
暗号文復号、
タイムスタンプ確認 (Sd3)
振込みが可能か
否かを判断 (Sd4)
計算値等のデータ
Sd5
電子署名検証、
暗号文復号、
タイムスタンプ確認
(Sd6)
データ表示し、
入力操作受付
(Sd7)
メッセージ
Sd8
電子バリュー
管理情報更新 (Sd9)
メッセージ
Sd10

【図１９】


MS
移動機
VM
自動
販売機
VS
自販機
サーバ
MN
移動通信網
EBS
電子銀行
サーバ